MHLW "Guidelines for the Security Management of Medical Information Systems version5 (May, 2017)"					Google Response
Item No	chapter	section	Guideline	Classification	
6.1-01	6	6.1	Develop and disclose policies on personal information protection.	minimum	N/A
6.1-02			The policy on safety management of information systems that handle personal information has been established. The policy should include at least the extent of information handled by information systems, how and how long they are handled and stored, ensuring that users are identified to prevent unnecessary and illegal accesses, the responsible person for safety management, and the contact point for complaints and questions.	minimum	Google is certified to the ISO27001 Standard, which regulates "Information Security Policy" (ISO 27001: 2013, Annex A.5) and Organization of Information Security (ISO27001:2013, Annex A.6). Information security oversight and management controls, including documentation of information security policies are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
6.2-01		6.2	All information handled by the information system must be listed.	minimum	N/A
6.2-02			The listed information should be classified according to the importance of safety management, and the information should be kept up-to-date at all times.	minimum	N/A
6.2-03			management this list so that the safety management personnel of the information system can confirm the list as soon as needed.	minimum	N/A
6.2-04			Performing risk analysis on the listed information.	minimum	N/A
6.2-05			The threats from this analysis should be addressed as shown in chapters 6.3 to 6.12.	minimum	N/A
6.2-06			Documented management of the above results.	Recommendation	N/A
6.3-01		6.3	Establish an information system administrator and restrict personnel in charge (including system management personnel). However, when the role is self-evident in small medical institutions, it is not necessary to define a clear rule.	minimum	Google is certified to the ISO27001 Standard, which regulates "Information Security Policy" (ISO 27001: 2013, Annex A.5) and Organization of Information Security (ISO27001:2013, Annex A.6). Information security oversight and management controls, including documentation of information security policies are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
6.3-02			Entry and exit management, such as recording and identifying visitors and restricting entry and exit, should be defined where personal data can be referenced.	minimum	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0
6.3-03			Create access management rules that define access restrictions, documents, inspections, etc. to information systems.	minimum	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
6.3-04			When commissioning the treatment of personal data, the commissioning agreement should include the terms of safety management.	minimum	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
6.3-05			Determine the following in the operation management regulations, etc. (a) Principles (Assertion of Basic Policies and management Objectives)	minimum	Google is certified to the ISO27001 Standard, which regulates "Documented Operating Procedures" (ISO27001:2013, Annex A.12.1.1). Google maintains robust internal documentation and maintains an ISMS, per ISO27001 requirements. All documentation in on systems that are replicated and subject to backup. Customers using Google Cloud Platform, retain all rights and responsibilities to configure and manage their environment, including development of operational guidance.
6.3-06			(b) Systems of medical institutions	minimum	Google is certified to the ISO27001 Standard, which regulates "Documented Operating Procedures" (ISO27001:2013, Annex A.12.1.1). Google maintains robust internal documentation and maintains an ISMS, per ISO27001 requirements. All documentation in on systems that are replicated and subject to backup. Customers using Google Cloud Platform, retain all rights and responsibilities to configure and manage their environment, including development of operational guidance.
6.3-07			(c) management of documents such as contracts and manuals	minimum	Google is certified to the ISO27001 Standard, which regulates "Documented Operating Procedures" (ISO27001:2013, Annex A.12.1.1). Google maintains robust internal documentation and maintains an ISMS, per ISO27001 requirements. All documentation in on systems that are replicated and subject to backup. Customers using Google Cloud Platform, retain all rights and responsibilities to configure and manage their environment, including development of operational guidance.
6.3-08			(d) Way to prevent risks and respond to incidents	minimum	Google is certified to the ISO27001 Standard, which regulates "Documented Operating Procedures" (ISO27001:2013, Annex A.12.1.1). Google maintains robust internal documentation and maintains an ISMS, per ISO27001 requirements. All documentation in on systems that are replicated and subject to backup. Customers using Google Cloud Platform, retain all rights and responsibilities to configure and manage their environment, including development of operational guidance.

MHLW "Guidelines for the Security Management of Medical Information Systems version5 (May, 2017)"					Google Response
Item No	chapter	section	Guideline	Classification	
6.3-09			(e) Equipment management when using the device	minimum	Google is certified to the ISO27001 Standard, which regulates "Documented Operating Procedures" (ISO27001:2013, Annex A.12.1.1). Google maintains robust internal documentation and maintains an ISMS, per ISO27001 requirements. All documentation in on systems that are replicated and subject to backup. Customers using Google Cloud Platform, retain all rights and responsibilities to configure and manage their environment, including development of operational guidance.
6.3-10			(f) management (storage, transfer, etc.) of personal-information recording media	minimum	Google is certified to the ISO27001 Standard, which regulates "Documented Operating Procedures" (ISO27001:2013, Annex A.12.1.1). Google maintains robust internal documentation and maintains an ISMS, per ISO27001 requirements. All documentation in on systems that are replicated and subject to backup. Customers using Google Cloud Platform, retain all rights and responsibilities to configure and manage their environment, including development of operational guidance.
6.3-11			(g) How to provide explanations and consent to the patient	minimum	N/A
6.3-12			(h) Auditing	minimum	Google provides contractual commitments related to audit rights. Please see Section 7.5.2 of the Data Processing and Security Terms (DPST) for GCP and Section 7.5.2 of the Data Processing Amendment (DPA) for G Suite.
6.3-13			(i) Contact point for complaints and questions	minimum	Google is certified to the ISO27001 Standard, which regulates "Documented Operating Procedures" (ISO27001:2013, Annex A.12.1.1). Google maintains robust internal documentation and maintains an ISMS, per ISO27001 requirements. All documentation in on systems that are replicated and subject to backup. Customers using Google Cloud Platform, retain all rights and responsibilities to configure and manage their environment, including development of operational guidance.
6.4-01		6.4	Lock the installation location of the equipment in which personal information is stored and the storage location of the recording medium.	minimum	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A. 11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers
6.4-02			In the quarters where a terminal capable of entry and referring to personal information is installed, measures such as locking other than business hours must be taken so that only authorized persons can access the terminal based on the operation management regulations. However, this is not the case if there are other possible means at the same level as this countermeasure item.	minimum	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0
6.4-03			Perform management to enter and leave the quarters where personal data is physically stored. For example, do the following: ・Enter and leave data by entering data in a ledger or the like. ・Periodically check and validate entry and exit records.	minimum	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0
6.4-04			Establish anti-theft chains for significant equipments such as PCs where personal information exists.	minimum	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A. 11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers
6.4-05			Implement measures to prevent peeping.	minimum	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A. 11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers

MHLW "Guidelines for the Security Management of Medical Information Systems version5 (May, 2017)"					Google Response
Item No	chapter	section	Guideline	Classification	
6.4-06			Installation of security cameras, automatic intrusion monitoring equipment, etc.	Recommendation	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0
6.5-01		6.5	Identify and authenticate users in accessing information systems.	minimum	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Access to information resources, including data and the systems which store or process data, is authorized based on the principle of least privilege. Access to network devices is authenticated via user ID, password, security key, and/or certificate. External system users are identified and authenticated via the Google Accounts authentication system before access is granted.
6.5-02			When a combination of a user ID and a password is used to identify and authenticate an individual, measures should be taken to keep such information known only to the individual.	minimum	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
6.5-03			When security devices such as IC cards are used to identify and authenticate individuals, temporary access rules should be prepared by alternative means in the event of an emergency, assuming that the identification information of the individuals cannot be used, such as damage to the IC cards.	minimum	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Both user and internal access to customer data is restricted through the use of unique user IDs. Access to sensitive systems and applications requires two-factor authentication in the form of a unique user ID, strong password, one-time password ("OTP"), security key, and/or certificates.
6.5-04			When an inputter leaves the terminal for a long time, if there is a risk of entry by someone other than the legitimate inputter, take precautions such as a clear screen.	minimum	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A. 11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers
6.5-05			When using data including personal information for operation confirmation, be careful about leakage, etc.	minimum	Google is certified to the ISO27001 Standard, which regulates "Separation of Development, Testing, and Operational Environments" (ISO 27001:2013, Annex A.12.1.4), " and Security in Development and Support Processes" (ISO 27001:2013, Annex A.14.2). Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
6.5-06			The extent of accessible medical records should be defined for each health care worker and job type relationship, and access management should be provided according to the levels. In addition, the operational management regulations specify that the access authorities should be reviewed as appropriate in accordance with changes in the user's assigned tasks due to personnel changes, etc. A system accessed by users of a plurality of job types is required to have an access management function for each job type. However, if such a function does not exist, it is necessary to establish an accessible range in terms of system updates and operational management regulations, and to ensure the accessible range by carrying out the operational records in the next section.	minimum	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
6.5-07			Record access and check logs on a regular basis. The record of access should be able to identify at least the login time of the user, the access time, and the patient operated during the login. It is premised that the information system has an access recording function. If not, it is necessary to record the operation (operator, operation content, etc.) in a business diary, etc.	minimum	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.

MHLW "Guidelines for the Security Management of Medical Information Systems version5 (May, 2017)"					Google Response
Item No	chapter	section	Guideline	Classification	
6.5-08			Restrict access to access logs to prevent unauthorized deletion, tampering, or addition of access logs.	minimum	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
6.5-09			Time information used for recording access must be reliable. Time information used inside medical institutions and the like must be synchronized, and precision of standard time and medical facts should be maintained in a range that does not cause problems by means of periodically matching the standard time.	minimum	Google is certified to the ISO 27001 Standard, which regulates "Clock Synchronisation" (ISO 27001: 20143, Annex 12.4.4) Google syncs all internal clocks to an atomic clocks and GPS and runs its own NTP service. Google makes it's Public NTP service available to customers via https://time.google.com
6.5-10			Check that unauthorized software, such as viruses, are not mixed when the system is built, when the media is not properly management, or when information is received from the outside. When using media that are not considered to be properly management, ensure adequate security and carefully use the media. Appropriate measures should be taken to prevent unauthorized software such as viruses from being constantly mixed. Confirmation and maintain the effectiveness and safety of the measures (e.g., check and maintain pattern file updates).	minimum	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001:2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/.
6.5-11			When Password is used for User Identification The systems management personnel should note the following: (1) In the password file in the system, the password is always encrypted (if possible, irreversible conversion is desired), and management and operation are performed in an appropriate manner. In addition, when other measures such as smart cards are used together to identify users, the operation management rules should specify how to operate passwords according to the systems. (2) If the user forgets the password or can be stolen, and the system management user changes the password, the user must be authenticated and the method used to verify the user's identity (attach copies of the document that has been authenticated) and re-register the password using a method that cannot be known by anyone other than the user. (3) Prevent measures that allow the user's password to be inferred even by the system management user (there must be no password in the configuration files, etc.). The user should also note the following: (1) Change passwords periodically (except when two-month authentication specified in D.5 is adopted for a maximum of two months). Do not use extremely short strings. A character string of eight or more characters in which alphanumeric characters and symbols are mixed is desirable. (2) Do not use passwords that are easy to guess, and do not use similar passwords repeatedly. Passwords that are easy to guess include their names, birth dates, and words listed in the dictionary.	minimum	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Users are required to authenticate using valid credentials prior to resetting their password. Passwords are managed in accordance with a set of password construction, protection and management guidelines, which enforce the following: a) Minimum length b) Complexity c) History d) Idle time lockout setting Password security requirements are stipulated in the security guidelines and controls (password complexity, expiration, etc.) are built into systems to help ensure that Google password standards are enforced.
6.5-12			Using the Radio LAN The systems management personnel should note the following: (1) The use of a wireless LAN should not be specified for users other than users. Take measures such as stealth mode and rejection of ANY connections. (2) Measures should be taken to prevent unauthorized access. Restrict accessing by at least SSID or MAC addresses. (3) Prevent unauthorized acquisition of information. Encrypting information and protecting data using, for example, a WPA2/AES. (4) Note that radio interference can occur depending on the equipment that generates radio waves (such as portable game consoles), so it should be used within medical institutions and other facilities. (5) Regarding the application of wireless LAN, refer to "To use wireless LAN with security" issued by MIC.	minimum	N/A
6.5-13			13. Using IoT Equipments The systems management personnel should note the following: (1) When the patient information is handled by the IoT device, the risk is analyzed on the basis of the information on the cyber security of the medical device provided by the manufacturer and seller, and the operation management regulations related to the treatment should be defined. (2) When lending wearable terminals or IoT devices installed at home, which are difficult to take adequate security measures, to the subject, explain information security risks to the subject in advance and obtain consent to the information security risks. Provide information to the patient about contact information and how to contact medical institutions when an abnormality or inconvenience occurs in the device. (3) In some cases, vulnerabilities related to firmware or the like are discovered in IoT equipments after the products are shipped. Consider and apply methods to properly perform security-critical updates of IoT equipments when needed, based on the characteristics of systems and services. (4) Measures should be taken to prevent unauthorized connections if IoT equipments whose use has been terminated or stopped due to problems are left connected to networks.	minimum	N/A
6.5-14			Perform information-category management and access management on a per-partition basis.	Recommendation	Google is certified to the ISO27001 Standard, which regulates "Information classification" (ISO 27001: 2013, Annex A.8.2). Information security oversight and management controls, including software development controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google has also developed the Data Security Policy, Data Classification Guidelines, and Security Labels for Google Information to establish procedures for information labeling and handling in accordance with the Google data classification guidelines. Policies and procedures are reviewed and updated as necessary.

MHLW "Guidelines for the Security Management of Medical Information Systems version5 (May, 2017)"					Google Response
Item No	chapter	section	Guideline	Classification	
6.5-15			Close processing etc. in case of absence (Clear screen: logoff or screen saver with password etc.)	Recommendation	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A. 11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers
6.5-16			Establish firewalls (including stateful inspection and equivalent functions) at points connected to external networks and critical parts of safety management, such as DB-servers, and appropriately set access-control lists (ACLs).	Recommendation	Google is certified to the ISO27001 Standard, which regulates "Network Controls" (ISO27001:2013, Annex A.13.1.1). Common criteria related to logical and physical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google employs multiple layers of network devices to protect its external attack surface. Google considers potential attack vectors and incorporates appropriate defensive controls at its perimeter and boundaries. Network ACLs are documented within configuration files with comments on purpose, as appropriate.
6.5-17			When passwords are used for user identification, the following standards must be observed. (1) Set a certain refractory time for re-entry when password entry is unsuccessful. (2) A mechanism shall be adopted in which re-entry is not accepted for a certain period of time when password re-entry fails more than a certain number of times.	Recommendation	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Users are required to authenticate using valid credentials prior to resetting their password. Passwords are managed in accordance with a set of password construction, protection and management guidelines, which enforce the following: a) Minimum length b) Complexity c) History d) Idle time lockout setting Password security requirements are stipulated in the security guidelines and controls (password complexity, expiration, etc.) are built into systems to help ensure that Google password standards are enforced.
6.5-18			As means used for authentication, a method with higher authentication strength, such as a method using two independent components (two-factor authentication) such as ID, password, biometrics, security device such as an IC card, password, or biometrics, should be adopted. However, even if two-factor authentication is not implemented in a terminal using an information system, it may be considered equivalent to two-factor authentication as long as two or more factors (any two or more of storage, biometric measurement, and physical media) are authenticated, including at the time of entry and at the time of use of the terminal, for example, by authenticating a user at the time of entry to a quarters operation the terminal.	Recommendation	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Both user and internal access to customer data is restricted through the use of unique user IDs. Access to sensitive systems and applications requires two-factor authentication in the form of a unique user ID, strong password, one-time password ("OTP"), security key, and/or certificates.
6.5-19			When a plurality of access points of a wireless LAN are installed and operated, the complexities of management may increase and the risk of intrusion may increase. When installing a device that raises the risks of such intrusion, for example, strengthen security by combining 802.1x and electronic certificates.	Recommendation	N/A
6.5-20			In order to grasp the connection status and abnormal occurrence of the system including the IoT equipment, IoT equipment and system should collect and grasp the respective status and the communication status with other equipment and record them appropriately as logs.	Recommendation	N/A
6.6-01		6.6	(1) Human Safety management Measures for Employees management personnel such as healthcare institutions must take actions to properly implement measures related to the safety management of personal data and oversee the status of the implementation, and the following measures must be taken. 1. When adopting persons other than those who have legal confidentiality obligations as administrative personnel, perform safety management by concluding a confidentiality/non-disclosure contract at the time of employment and contract.	minimum	Google is certified to the ISO27001 Standard, which regulates "Terms and Conditions of Employment" (ISO 27001:2013, Annex A.7.1.2), Hiring practices controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google performs background checks on new hires as permitted by local laws
6.6-02			2. Periodically train employees in the safety management of personal data.	minimum	Google is certified to the ISO27001 Standard, which regulates "Information Security Awareness, Education and Training" (ISO 27001:2013, Annex A.7.2.2), Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All Google contractors undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new contractors agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.
6.6-03			3. Define rules for protecting personal information after employee retirement.	minimum	Google is certified to the ISO27001 Standard, which regulates "Termination or change of Employment Responsibilities" (ISO 27001:2013, Annex A.7.3.11.2), Hiring practices controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Access to production machines, support tools, network devices, and corporate assets is automatically removed in timely basis upon submission of a termination request by the appropriate Googler.
6.6-04			In management significant locations, such as in server rooms, management of actions to employees should be conducted by monitoring, etc.	Recommendation	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0

MHLW "Guidelines for the Security Management of Medical Information Systems version5 (May, 2017)"					Google Response
Item No	chapter	section	Guideline	Classification	
6.6-05			When outsourcing services and operations of medical institutions to external operators, take the following measures to ensure proper protection of personal information within medical institutions. ① Enter a confidentiality agreement supported by business rules that set a comprehensive penalty for contracted operators.	minimum	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
6.6-06			② When directly accessing medical information systems such as maintenance work, confirm workers, work contents, and work results.	minimum	Google is certified to the ISO27001 Standard, which regulates ""Access Control"" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on their job function and role, using the concepts of least-privilege and need-to-know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and aan approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams.
6.6-07			③ Periodic checks should be made after the task even if the task does not access the medical information system directly, such as cleaning.	minimum	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0
6.6-08			④ Clear whether or not the consignor performs the re-consignment. When the re-consignment is performed, it is required that measures and contracts are made for the protection of personal information equivalent to those of the consignor.	minimum	Google is certified to the ISO27001 Standard, which regulates "Supplier Relationships" (ISO 27001:2013, Annex A.15). Information security oversight and management controls, including vendor security practices are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google directly conducts virtually all data processing activities to provide our services. However, Google may engage some third-party suppliers to provide services related to Cloud Platform, including customer and technical support. Prior to onboarding third-party suppliers, Google conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms.
6.6-09			When an external maintenance staff accesses personal information such as medical records for unwanted circumstances, such as when stored data needs to be rescued due to abnormalities in programs, etc., measures should be taken to maintain stealthy such as confidentiality agreements supported by penalized business rules, etc.	Recommendation	Google is certified to the ISO27001 Standard, which regulated "Supplier Relationships" (ISO 27001:2013, Annex A.15) Information security oversight and management controls, including vendor security practices are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google employs a vendor management process that includes contractual requirements to adhere to Google's security policies and onsite inspections, as needed, to confirm compliance.
6.7-01		6.7	「6.1 Establish and announce policies. Define procedures for destruction for each type of information identified in the Policy. The procedure should include the conditions under which the destruction is to be performed, the identification of employees who can perform the destruction, and the specific method of destruction.	minimum	Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" (ISO 27001:2013,Annex A.11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.
6.7-02			When discarding the information processing equipment itself, it must be done by someone with specialized knowledge, and it must be confirmed that there is no remaining and readable information.	minimum	Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" ((ISO 27001:2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" ((ISO 27001:2013,Annex A.11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.
6.7-03			When entrusting the discarding of datum to an external storage contractor, confirm that the information has been discarded surely by the entrusted medical institution, etc. in accordance with "6.6 Personnel Safety Measures (2) Supervision and Confidentiality Agreement of Administrative Agencies".	minimum	Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" ((ISO 27001:2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" ((ISO 27001:2013,Annex A.11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.
6.7-04			Determine the following in the Operation management Rules. (a) Creation of rules that govern the destruction of media containing personal information that is no longer needed	minimum	Google is certified to the ISO27001 Standard, which regulates "Information Security Policy" (ISO 27001:2013, Annex A.5) and Organization of Information Security (ISO27001:2013, Annex A.6). Information security oversight and management controls, including documentation of information security policies are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.

MHLW "Guidelines for the Security Management of Medical Information Systems version5 (May, 2017)"					Google Response
Item No	chapter	section	Guideline	Classification	
6.8-01		6.8	When data including personal information is used in operation confirmation, clear confidentiality obligations should be set, and it should be required to perform processing such as deleting data reliably after completion.	minimum	Google is certified to the ISO27001 Standard, which regulates "Separation of Development, Testing, and Operational Environments" (ISO 27001:2013, Annex A.12.1.4), " and Security in Development and Support Processes" (ISO 27001:2013, Annex A.14.2). Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
6.8-02			When a maintenance company worker accesses a server to perform maintenance, use a dedicated accounts of the maintenance personnel, and leave work records including whether or not to access personal information and, when accessing the server, the target personal information. This also applies to identifying and authentication for performing operation confirmation imitating a system user.	minimum	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
6.8-03			Require appropriate management of the accounts data from the viewpoint of preventing unauthorized use due to outflow, etc.	minimum	Google is certified to the ISO27001 Standard, which regulates "User access management" (ISO 27001: 2013, Annex A.9.2). Google restricts access based on need-to-know and job function. Google maintains automated log collection and analysis tools. An automated access revocation process exists that includes account locking and revocation of certificates and role assignment.
6.8-04			Maintenance accounts must be deleted promptly when maintenance personnel leave the office or change in responsibility, and a accounts management system must be established to respond to the deletion.	minimum	Google is certified to the ISO27001 Standard, which regulates "User access management" (ISO 27001: 2013, Annex A.9.2). Google restricts access based on need-to-know and job function. Google maintains automated log collection and analysis tools. An automated access revocation process exists that includes account locking and revocation of certificates and role assignment.
6.8-05			When a maintenance company performs maintenance, it is required to submit work requests in advance on a daily basis, and prompt the submission of a work report at the time of completion.	minimum	Google is certified to the ISO27001 Standard, which regulated "Supplier Relationships" (ISO 27001:2013, Annex A.15) Information security oversight and management controls, including vendor security practices are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google employs a vendor management process that includes contractual requirements to adhere to Google's security policies and onsite inspections, as needed, to confirm compliance.
6.8-06			These documents should be approved one by one by the administrator of the medical institution.	minimum	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
6.8-07			Enter a confidentiality agreement with a maintenance company to comply with the agreement. It should be avoided for maintenance companies to take data containing personal data out of the organization. However, when the data must be taken out of the organization under unavoidable circumstances, the administrator of the healthcare institution should approve the operation management regulations for handling including adequate measures against misplacement and the like one by one, and the administrator of the healthcare institution should approve it one by one.	minimum	Google maintains formal access procedures for allowing physical access to the data centers. The data centers are housed in facilities that require electronic card key access, with alarms that are linked to the onsite-site security operation. All entrants to the data center are required to identify themselves as well as show proof of identity to on-site secutity operations. Only authorized employees, contractors, and visitors are allowed entry to the data centers. Only authorized employees and contractors are permitted to request (which is followed by proper approval process) electronic card kay access to these facilities. Data center electronic card key access requests must be made through e-mail, and requires the approval of the requestor's manager and the data center director. All other entrants requiring temporary data center access must: (i) obtain approval in advance from the data center managers for the specific data center and internal areas they wish to visit, (ii) sign in at on-site security operations (iii) and reference an approved data center access record identifying the individual as approved.
6.8-08			When a system is modified or maintained by remote maintenance, access logs must be collected, and the responsible person at the medical institution must confirm the content of the operation immediately after the end of the operation.	minimum	Google maintains automated log collection and analysis tools that collect and correlate log information from various sources.
6.8-09			When a subcontract is performed, the same obligation must be imposed on the subcontractor at the maintenance company's responsibility.	minimum	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
6.8-10			Record detailed operation records as maintenance operation logs.	Recommendation	Google maintains automated log collection and analysis tools that collect and correlate log information from various sources.
6.8-11			Maintenance should be conducted in the presence of medical institutions or other related personnel during maintenance.	Recommendation	Google maintains a robust vendor management program. Vendors who work with Google are required to comply with all relevant information security and privacy policies. A vendor audit program is in place to determine compliance.
6.8-12			Request a confidentiality agreement between each worker and the maintenance company.	Recommendation	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
6.8-13			Maintenance companies should avoid taking data containing personal information out of the organization, but should require detailed work records to be kept if they must be taken out of the organization under unavoidable circumstances. In addition, it is required to respond to the audit of medical institutions, etc. as necessary.	Recommendation	Google is certified to the ISO27001 Standard, which regulates "Information Systems Audit Considerations" (ISO 27001:2013, Annex A.12.7). Information security oversight and management controls, including the establishment of internal audit oversight are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google maintains formal access procedures for allowing physical access to the data centers. The data centers are housed in facilities that require electronic card key access, with alarms that are linked to the onsite-site security operation. All entrants to the data center are required to identify themselves as well as show proof of identity to on-site secutity operations. Only authorized employees, contractors, and visitors are allowed entry to the data centers. Only authorized employees and contractors are permitted to request (which is followed by proper approval process) electronic card kay access to these facilities. Data center electronic card key access requests must be made through e-mail, and requires the approval of the requestor's manager and the data center director. All other entrants requiring temporary data center access must: (i) obtain approval in advance from the data center managers for the specific data center and internal areas they wish to visit, (ii) sign in at on-site security operations (iii) and reference an approved data center access record identifying the individual as approved.

MHLW "Guidelines for the Security Management of Medical Information Systems version5 (May, 2017)"					Google Response
Item No	chapter	section	Guideline	Classification	
6.8-14			As a means for checking logs related to maintenance work, a mechanism must be provided in which identification information of accessed medical records and the like is displayed in chronological order, and how many times access has been made to which patient within a specified time can be checked.	Recommendation	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
6.9-01		6.9	Perform risk-analysis as an organization, and define policies regarding the removal of information and information devices in the operation management rules.	minimum	Google is certified to the ISO27001 Standard, which regulates "Documented Operating Procedures" (ISO27001:2013, Annex A.12.1.1). Google maintains robust internal documentation and maintains an ISMS, per ISO27001 requirements. All documentation in on systems that are replicated and subject to backup. Customers using Google Cloud Platform, retain all rights and responsibilities to configure and manage their environment, including development of operational guidance.
6.9-02			The Operation management Regulations shall specify the management methods of the information and information devices taken out.	minimum	Google is certified to the ISO27001 Standard, which regulates "Documented Operating Procedures" (ISO27001:2013, Annex A.12.1.1). Google maintains robust internal documentation and maintains an ISMS, per ISO27001 requirements. All documentation in on systems that are replicated and subject to backup. Customers using Google Cloud Platform, retain all rights and responsibilities to configure and manage their environment, including development of operational guidance.
6.9-03			Response to theft/loss of information-carrying media or information devices should be specified in the Operation management Rules.	minimum	Google is certified to the ISO27001 Standard, which regulates "Documented Operating Procedures" (ISO27001:2013, Annex A.12.1.1). Google maintains robust internal documentation and maintains an ISMS, per ISO27001 requirements. All documentation in on systems that are replicated and subject to backup. Customers using Google Cloud Platform, retain all rights and responsibilities to configure and manage their environment, including development of operational guidance.
6.9-04			Ensure that employees are familiar with measures against thefts and losses specified in the Operation management Regulations and provide training.	minimum	Google is certified to the ISO27001 Standard, which regulates "Information Security Awareness, Education and Training" (ISO 27001:2013, Annex A.7.2.2), Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All Google contractors undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new contractors agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.
6.9-05			Medical institutions and information management personnel should grasp the location of portable media or information devices in which information is stored, for example, by using a register.	minimum	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001: 2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
6.9-06			Set a startup password or the like for the information device. In setting, measures should be taken to avoid the use of easy-to-estimate passwords, etc., and to change passwords periodically, etc.	minimum	N/A
6.9-07			As actions against theft, forgetting, etc., the contents should not be easily read, such as encryption of information or setting of an access password.	minimum	N/A
6.9-08			When information devices taken out are connected to a network or other external media are connected, measures should be taken to prevent information terminals from becoming subject to information leakage, tampering, etc. by introducing anti-computer virus software or using a personal firewall. When connecting to networks, follow the rules in Section 6.11, "Safety management when exchanging medical information including personal information with external devices". In particular, a public wireless LAN may be available on mobile devices such as smartphones and tablets, but the public wireless LAN may not meet the criteria of Section 6.5, C-11, and is therefore unavailable. However, use is permitted only in environments where only a public radio LAN is available. Select a communication method that meets the criteria described in Section 6.11.	minimum	N/A
6.9-09			Install only the minimum necessary applications on information devices that handle the information taken out. Delete or stop applications and functions that are not used for work, or confirm that there is no impact on work.	minimum	N/A
6.9-10			In cases where individual information devices (personal computers, smartphones, tablets, etc.) are to be handled by taking out information of medical institutions for business, the management must take measures from 1 to 5 and comply with the same requirements as in 6, 7, 8, and 9 in the responsibilities of management personnel.	minimum	N/A
6.9-11			To prevent information from being exposed by external peeping of information devices, a peeping prevention filter or the like should be provided on the display.	Recommendation	N/A
6.9-12			When logging in or accessing information from an information device, a combination of a plurality of authentication components should be used.	Recommendation	N/A

MHLW "Guidelines for the Security Management of Medical Information Systems version5 (May, 2017)"					Google Response
Item No	chapter	section	Guideline	Classification	
6.9-13			All portable media and information devices for storing information must be registered, and taking out of information by unregistered devices must be prohibited.	Recommendation	N/A
6.9-14			When a smartphone or tablet is taken out and used, the following measures should be taken. ・BYOD should not be performed in principle, and only the management person should be able to change the device settings. ・Do not place patient information in the terminal as much as possible in consideration of the possibility of loss or theft. If patient information is inevitably present in the terminal or if the patient information can be easily accessed by using the terminal, take measures such as initializing the terminal if the password is entered incorrectly a certain number of times.	Recommendation	N/A
6.10-01		6.10	A mechanism for judging "emergency" and procedures for returning to normal shall be provided as part of the BCP for continuing to provide medical services. In other words, standards, procedures, and judging persons for judging should be determined in advance.	minimum	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A. 17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
6.10-02			Prepare a convention for achieving data consistency between operations using alternative methods after returning to normal.	minimum	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A. 17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
6.10-03			Operation of information systems in emergency ・Maintain management procedures for emergency user accounts and emergency functions. ・Ensure that emergency functions are not inappropriately used at all times, and that, if used, management and auditing should be done appropriately, such as to make sure that many people know that they have been used. ・When emergency user accounts is used, change the setting so that continuous use is not possible after normal recovery. ・When medical information systems are infected with computer viruses due to targeted e-mail hit, etc., alternatives should be prepared, such as contacting relevant information or using paper.	minimum	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A. 17.2), and "Backup" (ISO27001:2013 Annex A 12.3.), and "Documented Operating Procedures" (ISO27001:2013, Annex A 12.1.1). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
6.10-04			In the event of problems in the system of providing medical services, such as the stoppage of some medical practices in a wide range of areas in the cyber hit, it should be judged as an "emergency" and be communicated to administrative authorities. Regardless of the above, if a medical information system fails, contact the authorities as necessary. Contact information: Health and Technology Information Promotion Office of Medical Development Department, Medical Department, Medical Department, Medical Department of Health and Labour Department (03-3595-2430) ※ In the case of independent administrative agencies, contact the supervisory department based on the information security policy of each corporation. The information processing promotion organization has established a window for receiving technical consultations regarding malware and unauthorized access. If someone receives targeted e-mail, Web sites are tampered with, unauthorized accesses, etc., the contact information below can be consulted. Information Security Consultation Center for Contact Information Processing Promotion Agency (03-5978-7509)	minimum	Google is certified to the ISO27001 Standard, which regulates "Access to Networks and Network Services" (ISO27001:2013, Annex A.9.1.2), "Network Security Management" (ISO27001:2013, Annex A.13.1). We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately.
6.11-01		6.11	Measures should be taken to prevent tampering such as message insertion and virus mixing on the network path. Measures should be taken to prevent password eavesdropping and body eavesdropping by crackers on routes between facilities. Measures should be taken to prevent spoofing such as session hijacking and IP address spoofing. As a measure to satisfy the above, for example, secure communication paths are secured by using a IPsec and a IKE. When configuring a network with the expectation of ensuring channel security in the adoption of a closed network, confirm to the operator the extent of the closed property of the service to be selected.	minimum	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001:2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/.

MHLW "Guidelines for the Security Management of Medical Information Systems version5 (May, 2017)"					Google Response
Item No	chapter	section	Guideline	Classification	
6.11-02			It is necessary to confirm the other party in the necessary units such as the entrance and exit of the base, the equipment in use, the functional units on the equipment in use, and the user at the data transmission source and the transmission destination. Determine which authentication to adopt based on the communication method to adopt and the operation management regulations. As the authentication means, it is desirable to use a method such as authentication by PKI, key distribution such as Kerberos, use of a shared key distributed in advance, a method such as one-time password which cannot be easily decrypted, and the like.	minimum	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
6.11-03			Measures should be taken in the facility to prevent spoofing of authorized users and spoofing of authorized equipments. This is described comprehensively in Section 6.5, "Technological Safety Measures" and is incorporated herein by reference.	minimum	N/A
6.11-04			Network devices such as routers must be routed so that they cannot be sent and received between VPN connecting different facilities through routers in the facilities using devices whose security can be checked. A device whose security can be confirmed refers to, for example, a device which can confirm that a document in which a security target defined by ISO15408 or a security measure similar to the security target is defined conforms to this guideline.	minimum	Google is certified to the ISO27001 Standard, which regulates "Access to Networks and Network Services" (ISO27001:2013, Annex A.9.1.2), "Network Security Management" (ISO27001:2013, Annex A.13.1). Google has dedicated teams who are responsible for monitoring, maintaining, managing, and securing the network. Connections to the corporate wireless network are encrypted.
6.11-05			Implement security measures such as encryption of the information itself between the source and destination parties. For example, measures such as the use of a SSL/TLS, the use of a S/MIME, and the encryption of files can be considered. In this case, the encryption key of the e-Government recommended encryption should be used.	minimum	Google is certified to the ISO27001 Standard, which regulates "Cryptography" (ISO 27001:2013, Annex A. 10) Encryption is used to protect user authentication and administrator sessions transmitted over the Internet. Remote access to Google corporate machines requires a Google issued digital certificate installed on the connecting device and two-factor authentication. Google publishes details about encryption and key management options for its Google Cloud Platform and G Suite products. To read more about key management and encryption, please see: https://cloud.google.com/security/encryption-at-rest/ https://cloud.google.com/security/encryption-in-transit/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including development of appropriate encryption measures.
6.11-06			Information communication between medical institutions and the like is related not only to medical institutions, but also to many organizations such as communication carriers, system integrators, operation consigned operators, equipment maintenance companies that perform remote maintenance, and the like. For this reason, in terms of the following matters, the responsibility division points of these related organizations and the locations of the responsibilities should be clarified in contracts, etc. ・Determining when to send medical information, including medical information, to a destination medical institution, etc. and the action to initiate a series of operations for exchanging information ・Measures to be taken when the sender's medical institution cannot connect to the network ・Measures to be taken when the destination medical institution is unable to connect to the network ・Response to the case where the route of the network is interrupted or significantly delayed. ・Measures to be taken when the stored information received by the destination medical institution, etc., cannot be received correctly ・To cope with problems in encrypting transmitted information ・Measures to be taken when there is a problem with the certification of the sender's medical institution and the recipient's medical institution ・Responsibility to isolate the failed part in the event of a disability ・Measures to be taken when the sender medical institution or recipient medical institution discontinues the exchange of information In addition, contract and operation management regulations should be set in the following items in the healthcare institution. ・Clarify of management responsibilities for communication devices, encryption devices, authentications, etc. When outsourcing management to external operators, the contract is concluded with the arrangement including the responsibilities division point. ・Clarify accountability for patient, etc. ・Establishment of dedicated management personnel to recover from accidents and communicate with other facilities and vendors. ・Clarify of management responsibilities and post-responsibilities for exchanged medical-information, etc. Items related to contact of the source and destination medical institutions when inquiries are received from the patient regarding the treatment of personal information, and stealthy items related to the handling of personal information in such cases.	minimum	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
6.11-07			When remote maintenance is performed, unnecessary log-in should be prevented by setting appropriate access points, restricting protocols, management access rights, etc. as needed. Refer to "6.8 Modification and Maintenance of Information Systems" for the maintenance itself.	minimum	Google is certified to the ISO27001 Standard, which regulates "Access to Networks and Network Services" (ISO27001:2013, Annex A.9.1.2), "Network Security Management" (ISO27001:2013, Annex A.13.1). Google has dedicated teams who are responsible for monitoring, maintaining, managing, and securing the network. Connections to the corporate wireless network are encrypted.
6.11-08			When signing agreements with line operators and on-line service providers, check the scope of management responsibilities against threats and quality-related issues such as line availability. Confirm that the above 1 and 4 are satisfied.	minimum	Google is certified to the ISO27001 Standard, which regulates "Communications Security" (ISO 27001:2013, Annex A.13), and "Securing Application Service on Public Networks" ISO 27001:2013, (Annex A. 14.1.2). Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including management of external connections.

MHLW "Guidelines for the Security Management of Medical Information Systems version5 (May, 2017)"					Google Response
Item No	chapter	section	Guideline	Classification	
6.11-09			When information is browsed by a patient, the system and applications should be separated through the computer system on which the information is published so that unauthorized intrusion does not occur in the system inside the medical institution, etc., and measures should be implemented using technologies such as firewalls, access monitoring, TLS-encryption of communication, PKI individual identification, etc. In addition, a satisfactory explanation of the risk and the purpose of provision should be given to the subject of information, and a wide range of measures should be taken, including legal rationales other than IT, to clarify the responsibilities of each.	minimum	Google is certified to the ISO27001 Standard, which regulates "Access to Networks and Network Services" (ISO27001:2013, Annex A.9.1.2), "Network Security Management" (ISO27001:2013, Annex A. 13.1). Google forces TLS for all authentication traffic. Customer data is encrypted when on Google's internal networks, in transport and at rest.
6.11-10			When establishing a connection using the HTTPS via an open network, the SSL/TLS protocol version should be limited to TLS 1. 2 only, unless security is guaranteed by VPN connection using IPsec, and then TLS client authentication using client certificates should be performed. In this case, both the server and the client should set the TLS appropriately according to the "high-security type" with the highest security level specified in the "SSL/TLS Cryptography Setting Guidelines". In principle, the so-called SSL-VPN should not be used because many countermeasures against fake servers are insufficient. In addition, when connecting by software-based IPsec or TLS1. 2, appropriate measures should be taken to protect against hit such as congestion between sessions (access to closed sessions that are not legitimate routes).	minimum	Google is certified to the ISO27001 Standard, which regulates "Communications Security" (ISO 27001: 2013, Annex A.13), and "Securing Application Service on Public Networks" ISO 27001:2013, (Annex A. 14.1.2). Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including management of external connections.
6.11-11			When permitting external accesses by employees, use technologies such as virtual desktops that combine virtual secure management environments with VPN technologies and set operational requirements.	Recommendation	Google is certified to the ISO27001 Standard, which regulates ""Access to Networks and Network Services"" (ISO27001:2013, Annex A.9.1.2), ""Network Security Management"" (ISO27001:2013, Annex A.13.1). Google segregates its production and corporate environments with appropriate network boundary controls.
6.12-01		6.12	(1) Digital signatures shall be provided using electronic certificates issued by the Medical and Welfare Field PKI Certification Authority or certified certification operators that meet the compliance auditing standards set by the MHLW. 1. The health care field PKI certificate authority stores the qualifications related to health care welfare, such as doctors, in an electronic certificate, and is constructed as an authentication base for certifying the qualifications. Therefore, it is recommended to use electronic signatures issued by this Healthcare Welfare Field PKI Certificate Authority. However, it is necessary that all persons who must verify the electronic signature be able to correctly verify the electronic signature including the national qualification.	minimum	N/A
6.12-02			2. Although it is possible to satisfy the requirement of A without using an electronic certificate issued by a certification-specific certification business operator based on the regulations of the electronic signature method, it is necessary to perform identity verification with equal strictness, and further to enable an administrative organization or the like to perform monitoring or the like to verify the electronic signature.	minimum	N/A
6.12-03			3. Pursuant to the Act on Certification Services of Local Public Entities Related to Electronic Signatures (Act No. 153 of 2002), it is also possible to use the Public Personal Certification Service, which has been launched since January 29, 2004, but in such a case, it is necessary for all persons who have to verify the electronic signature other than administrative organs to be able to verify the electronic signature using the Public Personal Certification Service.	minimum	N/A
6.12-04			(2) A time stamp should be attached to an entire document including an electronic signature. 1. The time stamp shall conform to the standards of the time authentication operation described in "Guidelines for Time Business-for safe use of networks and safe long-term storage of electronic data" (MIC, November 2004) and the third party shall be able to verify the time stamp using those of time certification operators certified by the Japan Data Communications Association.	minimum	N/A
6.12-05			2. Measures should be taken to maintain the validity of the time stamp during the statutory retention period.	minimum	N/A
6.12-06			3. With regard to the use of time stamps and long-term storage, it is necessary to take appropriate measures while paying attention to the contents of notifications and guidances of related government ministries, standard technologies, and related guidelines in the future.	minimum	N/A
6.12-07			(3) A valid digital certificate should be used when the time stamp is given. 1. Naturally, an electronic signature must be made using a valid electronic certificate. Although it is required that the electronic signature itself can be verified for the legal retention period, if the time stamp can be verified, it is proved that there is no fact of modification including the digital signature, and therefore, if the digital signature can be verified at the time of time stamping, the validity at the time of digital signature assignment can be verified. Specifically, while the electronic signature is valid, it is necessary to collect information (related electronic certificates, revocation information, and the like) necessary for verification of the electronic signature, and add a time stamp to the entire document to be signed and the signature value.	minimum	N/A
7.1-01	7	7.1	[Storage in medical institutions] (1) Identification and Authentication of Inputters and Confirmators a.When a record is created by a general-purpose input terminal such as a PC using an electronic medical record system or the like 1. To correctly identify and authenticate the inputter and confirmer.	minimum	Cloud Identity & Access Management (Cloud IAM) lets administrators authorize who can take action on specific resources, giving you full control and visibility to manage cloud resources centrally. For established enterprises with complex organizational structures, hundreds of workgroups, and potentially many more projects, Cloud IAM provides a unified view into security policy across your entire organization, with built-in auditing to ease compliance processes. IAM access policies are defined at the project level using granular controls of users and groups or using ACLs.
7.1-02			2. Define authorization management (access control) for all input operations to the systems based on required categories such as job type and department of the input person for each target data. To prevent creation, addition, and modification by anyone other than an authorized entry person.	minimum	Cloud Identity & Access Management (Cloud IAM) lets administrators authorize who can take action on specific resources, giving you full control and visibility to manage cloud resources centrally. For established enterprises with complex organizational structures, hundreds of workgroups, and potentially many more projects, Cloud IAM provides a unified view into security policy across your entire organization, with built-in auditing to ease compliance processes. IAM access policies are defined at the project level using granular controls of users and groups or using ACLs.
7.1-03			3. To management a terminal capable of operating a business application and prevent unauthorized users from accessing the terminal.	minimum	Cloud Identity & Access Management (Cloud IAM) lets administrators authorize who can take action on specific resources, giving you full control and visibility to manage cloud resources centrally. For established enterprises with complex organizational structures, hundreds of workgroups, and potentially many more projects, Cloud IAM provides a unified view into security policy across your entire organization, with built-in auditing to ease compliance processes. IAM access policies are defined at the project level using granular controls of users and groups or using ACLs.

MHLW "Guidelines for the Security Management of Medical Information Systems version5 (May, 2017)"					Google Response
Item No	chapter	section	Guideline	Classification	
7.1-04			b.When a record is created by a specific device or system, such as a Clinical Inspection System or a Medical Image Filing System 1. The management manager and operator of the machinery are clarified in the operation management regulations, and the operation of the equipment by persons other than the management manager and operator of the equipment is prevented in operation.	minimum	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A. 11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers
7.1-05			2. Recording by the device should be clear when and by whom it was done by a combination of system functions and operations.	minimum	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment.
7.1-06			(2) Establishment of procedures for establishing records and records of identification information of the person responsible for creation a.When a record is created by a general-purpose input terminal such as a PC using an electronic medical record system or the like 1. When creating and storing medical records, the system shall provide a mechanism for registering fixed information. In this case, identification information such as the name of the person in charge of creation and the date and time of creation using a reliable time source must be included.	minimum	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
7.1-07			2. Ensure that sufficient confirmation of the contents by the person responsible for the preparation is performed when confirming the records.	minimum	N/A
7.1-08			3. "Defined record" must be performed by a determinant who has authority to perform the confirmation.	minimum	N/A
7.1-09			4. Measures should be taken to prevent accidental entry, rewriting, deletion, and confusion of established records, and procedures for original state restoration should be examined.	minimum	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A. 17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing a process to support data file management activities.
7.1-10			5. For operations in which records are automatically established after a certain period of time, clear rules for specifying the input person and the confirmation person should be formulated and specified in the operation management rules.	minimum	N/A
7.1-11			6. If the confirmer cannot perform confirmation operations for some reason, the operation management regulation shall specify rules such as, for example, that the management manager of the healthcare institution will confirm the documents and clarify the location of the responsibilities for confirmation of the records.	minimum	N/A
7.1-12			b.When a record is created by a specific device or system, such as a Clinical Inspection System or a Medical Image Filing System 1. An operation management rule or the like defines a determination rule for records created by the device. In this case, identification information such as the name of the management responsibility or operator of the device (or identification information of the device), and the date and time of creation using a reliable time source should be included in the records.	minimum	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.

MHLW "Guidelines for the Security Management of Medical Information Systems version5 (May, 2017)"					Google Response
Item No	chapter	section	Guideline	Classification	
7.1-13			2. Measures should be taken to prevent accidental entry, rewriting, deletion, and confusion of established records, and procedures for original state restoration should be examined.	minimum	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A. 17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing a process to support data file management activities.
7.1-14			(3) Save Update History 1. When a medical record or the like that has been finalized once is updated, the update history can be saved, and the contents before and after the update can be collated as necessary.	minimum	Google maintains automated log collection and analysis tools that collect and correlate log information from various sources.
7.1-15			2. References should be made so that the order of updates can be identified when updates are made to the same medical record or the like multiple times.	minimum	Google monitors its access lists carefully to minimize the potential for unauthorized account use. Google periodically reviews access lists and removes access that is no longer required. All account actions are recorded.
7.1-16			(4) Authorization function for proxy entry 1. When performing proxy entry, the operation management regulations specify which tasks are specifically applied, and who can substitute whom.	minimum	N/A
7.1-17			2. When a proxy entry is made, the management of who and when the proxy was made is recorded each time the proxy entry is made.	minimum	Cloud Identity & Access Management (Cloud IAM) lets administrators authorize who can take action on specific resources, giving you full control and visibility to manage cloud resources centrally. For established enterprises with complex organizational structures, hundreds of workgroups, and potentially many more projects, Cloud IAM provides a unified view into security policy across your entire organization, with built-in auditing to ease compliance processes. IAM access policies are defined at the project level using granular controls of users and groups or using ACLs.
7.1-18			3. Records recorded by proxy entry should be subjected to "confirmation operation (approval)" by the confirmer as soon as possible. At this time, the confirmation operation must not be performed without confirming the contents.	minimum	N/A
7.1-19			(5) Quality management of equipment and software 1. It is clear what kind of equipment and software make up the system and what kind of scenes and applications it is used in, and the specifications of the system are clearly defined.	minimum	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001: 2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
7.1-20			2. A process for verifying the validity of the revision history of equipment and software and the work actually performed at the time of implementation thereof must be defined.	minimum	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001: 2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
7.1-21			3. Implement work content on quality management of equipment and software in the operation management regulations to educate employees, etc.	minimum	Google is certified to the ISO27001 Standard, which regulates "Information Security Awareness, Education and Training" (ISO 27001:2013, Annex A.7.2.2), Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All Google contractors undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new contractors agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.
7.1-22			4. Periodically perform internal audits of system configuration and software operational status.	minimum	Google maintains an internal audit program consistent with industry best practices and regulatory requirements. Google's corporate Internal Audit team covers multiple disciplines and operational aspects of Google, including cross-functional audit of assessments.
7.1-23			[To save data outside medical institutions through a network] In addition to the minimum guidelines for storage in medical institutions, the following items are required. (1) A mutual authentication function is required to recognize whether a medical institution or the like entrusted with online external storage such as a medical record performs mutual authentication for recognizing that a communication partner is legitimate, and whether the medical institution or the like entrusted with online external storage of the medical record or the like is a legitimate partner for mutual communication purposes.	minimum	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment.

MHLW "Guidelines for the Security Management of Medical Information Systems version5 (May, 2017)"					Google Response
Item No	chapter	section	Guideline	Classification	
7.1-24			(2) To ensure that they have not been "tampered with" on the network It must be possible to ensure that the medical record or the like has not been tampered with during the transfer of the network. It should be noted that lossless compression and decompression of information, tagging for ensuring security, encryption, decryption, and the like are not tampering.	minimum	Google is certified to the ISO27001 Standard, which regulates "Logging and Monitoring" (ISO 27001:2013, Annex A.12.4). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's security monitoring program is focused on information gathered from internal network traffic, employee actions on systems and outside knowledge of vulnerabilities. At many points across our global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections. This analysis is performed using a combination of open-source and commercial tools for traffic capture and parsing. A proprietary correlation system built on top of Google technology also supports this analysis. Network analysis is supplemented by examining system logs to identify unusual behavior, such as attempted access of customer data. Google security engineers place standing search alerts on public data repositories to look for security incidents that might affect the company's infrastructure. They actively review inbound security reports and monitor public mailing lists, blog posts, and wikis. Automated network analysis helps determine when an unknown threat may exist and escalates to Google security staff, and network analysis is supplemented by automated analysis of system logs. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuration of specific monitoring to detect false or unverified data.
7.1-25			(3) Restricting Remote Login Functionality A function must be provided to restrict the remote login to an adequately management so that it cannot be performed unless it is necessary for maintenance purposes or the like. For details of these requirements, see Section 6.11, "Safety management for Interchange of Medical Information with External Medical Information."	minimum	Google is certified to the ISO27001 Standard, which regulates "Access to Networks and Network Services" (ISO27001:2013, Annex A.9.1.2), "Network Security Management" (ISO27001:2013, Annex A.13.1). Access to information resources, including data and the systems which store or process data, is authorized based on the principle of least privilege. Access to network devices is authenticated via user ID, password, security key, and/or certificate. External system users are identified and authenticated via the Google Accounts authentication system before access is granted.
7.2-01		7.2	(1) Location management All the locations of information on a patient-by-patient basis must be routinely management, even if the information is distributed management to various media, including information on paper management.	minimum	N/A
7.2-02			(2) management of reading tools All information stored on electronic media and the means of reading the information are management in association with each other. In addition, equipment, software, and related information, which are reading means, must be maintained at all times.	minimum	N/A
7.2-03			(3) Response time for reading purposes It should be possible to promptly display on a search display or a document according to the purpose.	minimum	N/A
7.2-04			(4) Ensuring redundancy as a measure against system failures In order to make it possible to read medical records and the like within the extent where normal medical care or the like is allowed even when a disability occurs in one system of the system, redundancy of the system (to prepare and operate spare equipment such as servers and network equipment from the usual time in order to maintain the function of the whole system even when a failure occurs), or to prepare alternative reading means.	minimum	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A. 17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
7.2-05			[Storage in medical institutions] (1) Backup server Even when the system is stopped, the backup server and the general-purpose browser can be used to read the minimum medical records necessary for daily medical care.	Recommendation	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A. 17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing a process to support data file management activities.
7.2-06			(2) External output to ensure readability Even when the system is stopped, a series of medical records of the patient corresponding to the reading purpose can be output to an external file in a format that ensures readability so that the patient can be read with a general-purpose browser or the like.	Recommendation	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A. 17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing a process to support data file management activities.

MHLW "Guidelines for the Security Management of Medical Information Systems version5 (May, 2017)"					Google Response
Item No	chapter	section	Guideline	Classification	
7.2-07			(3) Reading function using remote data backup As a countermeasure against a disaster such as a large-scale fire, the electronic archive record should be backed up in a remote location, and the minimum medical record necessary for daily medical care can be read using the backup data and a general-purpose browser.	Recommendation	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A. 17.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions.
7.2-08			[To save data to the outside via a network] In addition to the recommended guidelines for storage in medical institutions, the following items are required. (1) Ensuring readability of medical records expected to be urgently needed Records that are expected to be urgently needed should be stored internally or, even if stored externally, duplicated or equivalent data should be retained internally at medical institutions.	Recommendation	N/A
7.2-09			(2) Ensuring readability of medical records that are not required to be urgent Actions should be taken to cope with failures in the network and external storage institutions, even for information that is not necessary until it is urgently needed.	Recommendation	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A. 17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing a process to support data file management activities.
7.3-01		7.3	[Storage in medical institutions] (1) Prevention of information destruction and confusion by viruses and inappropriate software 1. management of software, equipment, and media used in systems so as not to destroy or confuse information by inappropriate software including so-called computer viruses.	minimum	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001:2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/.
7.3-02			(2) Prevention of loss and destruction of information due to inappropriate storage and handling 1. Prepare operational management regulations for storage and handling of recording media and recording equipment, and educate relevant personnel for proper storage and handling, to ensure thorough dissemination. In addition, a history of work related to storage and handling should be kept.	minimum	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001: 2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
7.3-03			2. Specify the location (internal, portable medium) where the system stores the information, and specify the storable amount (size, period), risk, response, backup frequency, backup method, etc. for each location. These should be compiled as operation management regulations, and the operation should be made well known to all parties concerned.	minimum	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A. 17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing a process to support data file management activities.

MHLW "Guidelines for the Security Management of Medical Information Systems version5 (May, 2017)"					Google Response
Item No	chapter	section	Guideline	Classification	
7.3-04			3. Measures should be taken to prevent only authorized persons from entering the storage location of the recording medium or the server.	minimum	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0
7.3-05			4. Keep a history of access to electronically stored medical records and other information and management the history of access to the information.	minimum	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
7.3-06			5. When the information in each storage location fails, the backup data should be used to restore the state before the failure. If you are unable to return to the same position as before the loss, make it easier to identify the impaired range.	minimum	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A. 17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing a process to support data file management activities.
7.3-07			(3) Preventing information from being unreadable or incompletely read due to deterioration of recording media and facilities 1. Copying information to a new recording medium or equipment before the recording medium is degraded. Clear the period during which data can be normally stored without deterioration for each recording medium and equipment. management the start date of use and the end date of use, check the data about once a month, and copy the data to a new recording medium or device for which the end date of use is approaching. The flow of these operations should be summarized in the Operation management Rules and made well known to the relevant personnel.	minimum	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A. 17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing a process to support data file management activities.
7.3-08			(4) Preventing information from being unrecoverable due to inconsistencies in media, equipment, and software 1. In order to enable quick transition during system update, the function shall be provided to output and input data such as medical records in a standard format for items having a standard format, and in a data format that is easy to convert for items having no standard format.	minimum	Google is certified to the ISO27001 Standards, which regulates "Operational Procedures and Responsibilities" (ISO 27001:2013, Annex A.12.1) and "Network Security" (ISO 27001:2013, Annex A. 13.1). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. System changes that may affect security, availability, processing integrity, or confidentiality are communicated to management and users who will be affected.
7.3-09			2. The Master Database shall be equipped with a function that prevents changes in the contents of datum such as past medical records from occurring when the Master Database is changed.	minimum	Google is certified to the ISO27001 Standard, which regulates "Logging and Monitoring" (ISO 27001:2013, Annex A.12.4). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report.
7.3-10			[To save data outside medical institutions through a network] In addition to the minimum guidelines for storage in medical institutions, the following items are required. (1) management of versions and continuity of data formats and transport protocols It is conceivable that the data format and the transfer protocol are upgraded or changed during the period in which the storage obligation exists. In this case, the institution which accepts the external storage must maintain the correspondence while the medical institution which uses the former data format or transfer protocol exists.	minimum	Google is certified to the ISO27001 Standards, which regulates "Operational Procedures and Responsibilities" (ISO 27001:2013, Annex A.12.1) and "Network Security" (ISO 27001:2013, Annex A. 13.1). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. System changes that may affect security, availability, processing integrity, or confidentiality are communicated to management and users who will be affected.

MHLW "Guidelines for the Security Management of Medical Information Systems version5 (May, 2017)"					Google Response
Item No	chapter	section	Guideline	Classification	
7.3-11			(2) Measures should be taken to prevent deterioration of equipments of institutions that receive requests for network and external storage. Consider the terms of the network and the facilities of the institution that accepts external storage, and take measures such as updating the lines and facilities when they deteriorate.	minimum	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A. 17.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
7.3-12			[Storage in medical institutions] (1) Prevention of loss and destruction of information due to inappropriate storage and handling 1. Storage of recording media, recording equipments, and servers should be kept in a room where only authorized persons can enter, and the history of entering and leaving the room should be kept in association with the work history related to storage and handling.	Recommendation	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google’s focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0
7.3-13			2. Take physical measures, such as keys, to prevent only authorized users from entering the server room.	Recommendation	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google’s focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0
7.3-14			3. Provide a function to periodically acquire backups of data such as medical records and check that the contents of the backups have not been destroyed due to tampering or the like.	Recommendation	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored, logged and periodically approved for appropriateness. Employees with access must follow documented policies and procedures for the type of secured areas they are working in.
7.3-15			(2) Preventing information from being unreadable or incompletely read due to deterioration of recording media and facilities When information such as medical records is stored in a recording device such as a hard disk, countermeasures should be taken against RAID-1 or disk failure corresponding to a RAID-6 or more.	Recommendation	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A. 17.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
7.3-16			[To save data outside medical institutions through a network] (1) Ensuring compatibility of network and external storage facilities 1. When a line or equipment is updated to a new one, equipment corresponding to an old system becomes difficult to obtain, and reading recorded information may be disturbed. Therefore, organizations that accept external storage must ensure future compatibility when selecting lines and equipments, and must migrate to compatible lines and facilities that can cope with legacy systems and ensure safe data storage when updating the system.	Recommendation	Google is certified to the ISO27001 Standards, which regulates "Operational Procedures and Responsibilities" (ISO 27001:2013, Annex A.12.1) and "Network Security" (ISO 27001:2013, Annex A. 13.1). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. System changes that may affect security, availability, processing integrity, or confidentiality are communicated to management and users who will be affected.
8.1-01	8	8.1	① Storage in locations where hospitals, clinics, medical institutions, etc. properly management (a) Store the medical record inside the hospital or clinic.	minimum	N/A
8.1-02			(b) Do not treat records for the purpose of analysis, etc. without permission of hospitals, clinics, and patient who have entrusted storage.	minimum	N/A

MHLW "Guidelines for the Security Management of Medical Information Systems version5 (May, 2017)"					Google Response
Item No	chapter	section	Guideline	Classification	
8.1-03			(c) In the case where a hospital, a clinic, or the like analyses a medical record or the like for which storage has been commissioned, it is only necessary to obtain consent from the commissioned hospital, the clinic, and the patient and not to obtain an illegal income or benefit.	minimum	N/A
8.1-04			(d) Even when anonymous information is handled, the verification organization must examine the validity of anonymization and notify the patient of the fact that the anonymization is handled by using bulletins, etc. in consideration of the protection of personal information.	minimum	N/A
8.1-05			(e) When providing a mechanism for the patient to access the institution where the information is stored and browse his/her records, the hospitals and clinics entrusted with the storage of the information must specify appropriate access rights to ensure that information leakage or erroneous browsing (such as showing information of different patient or showing information that should not be shown to the patient) does not occur.	minimum	N/A
8.1-06			(f) Provision of information should be performed in principle by agreement between the medical institution and the patient where the patient is receiving the information.	minimum	N/A
8.1-07			② Storage in data centers established by government organizations (a) The laws and regulations specify the prohibition of confidentiality, unauthorized use, etc. of the content of personal information for individuals engaged in preservation work or individuals engaged in preservation work, and the penalty is applied due to breach of the regulations.	minimum	N/A
8.1-08			(b) Periodically verify that you have the required technologies and operational management capabilities for proper external storage, such as being audited by auditors with proper capabilities, such as systems audit technicians and Certified Information Systems Auditor (ISACA certification.	minimum	N/A
8.1-09			(c) The medical institution, etc. shall confirm that the information stored is not analyzed or analyzed by the external contractor, and shall exchange a contract, etc. stating that the information is not to be executed.	minimum	N/A
8.1-10			(d) Medical institutions must specify provision of information in contract forms, etc. so that the operator who accepts external storage does not provide the stored information independently. When establishing access privileges for external storage, the operator should set appropriate privileges to prevent information leakage or erroneous browsing (such as showing information of different patient or seeing information that should not be shown to patient).	minimum	N/A
8.1-11			③ When medical institutions store data in safe locations secured based on contracts with private operators, etc. (a) A medical institution must be able to manage the treatment of stored data by exchanging a contract with a provider who accepts external storage, including items related to confidentiality and penalties in the event of violations to the management operator or electronic storage worker.	minimum	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
8.1-12			(b) "6.11 Safety management when exchanging medical information, including personal information, with external organizations" must be observed for the safety of networks connecting medical institutions, etc. and businesses that are entrusted with external storage.	minimum	N/A
8.1-13			(c) management of medical-information from the METI, which is assigned to private operators by consigned operators. Clearly specify that the Guidelines for Information Processing Operators, the Guidelines for Information Security Measures in ASP and SaaS by MIC, and the Guidelines for Safety management when ASP and SaaS Operators Handle Medical Information, etc. are to be adhered to, and confirm by receiving reports at least periodically.	minimum	Google is certified to the ISO27001 Standard, which regulates "Supplier Relationships" (ISO 27001:2013, Annex A.15). Information security oversight and management controls, including vendor security practices are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google directly conducts virtually all data processing activities to provide our services. However, Google may engage some third-party suppliers to provide services related to Cloud Platform, including customer and technical support. Prior to onboarding third-party suppliers, Google conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms.
8.1-14			(d) Stored information must not be viewed beyond the scope required for maintenance work within the scope of contract exchanged by operators who accept external storage. For maintenance, observe Section 6.8, "Modification and Maintenance of Information Systems".	minimum	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
8.1-15			(e) Do not analyze or analyze information stored by an operator who accepts external storage. The same applies to anonymized information. Specify these items in the contract and strictly adhere to them at medical institutions, etc.	minimum	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
8.1-16			(f) Medical institutions must specify provision of information in contracts, etc. so that a provider who accepts external storage does not independently provide the stored information. When establishing access privileges for external storage, the operator should set appropriate privileges to prevent information leakage or erroneous browsing (such as showing information of different patient or seeing information that should not be shown to patient).	minimum	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
8.1-17			(g) Establish criteria for selection of operators who accept external storage after satisfying (a) to (f) at medical institutions, etc. Check at least the following four points. (a) Development of basic policies and handling regulations related to safety management of medical-information, etc. (b) Establishment of an implementation system related to safety management of medical-information, etc... (c) Credentials for Personal Data Safety management Based on Actual Data, etc.... (d) Soundness of management based on financial statements, etc.	minimum	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
8.1-18			(a) In the case of "1) storage in a place where hospitals, clinics, medical corporations, etc. properly management", when storage is stored in a place where medical corporations, etc. properly management, a third party certification, such as privacy marking or ISMS certification, which is a certification system for protecting personal information and information security management, shall be obtained as a means of showing patients and citizens more self-help efforts as a whole of the organization that has entrusted the storage.	Recommendation	N/A

MHLW "Guidelines for the Security Management of Medical Information Systems version5 (May, 2017)"					Google Response
Item No	chapter	section	Guideline	Classification	
8.1-19			(b) "②In the case where the data is stored in a data center established by an administrative organization" or the like, it is to be monitored and evaluated in the system. However, as part of further evaluation, it is to be certified by a third party as described in (a).	Recommendation	N/A
8.1-20			(c) "②In the case where the data is stored in a data center established by an administrative organization" and "the case where the data is stored in a safe place secured by a medical institution or the like based on a contract with a private business operator", as a general rule, ensure that only the medical institution or the like to which the data is entrusted can view the data content, except for emergency measures such as data restoration work in the event of a trouble, for example.	Recommendation	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
8.1-21			(d) Encryption and appropriate management of personal identification-related information stored in operators who entrust external storage, and control mechanisms that are not normally accessible to management operators who entrust external storage. Specifically, methods of "encrypting" and "distributing and storing information" are considered. In this case, access should be assumed under circumstances different from normal conditions such as emergency, and a mechanism should be provided to allow medical institutions to explicitly identify the fact of access.	Recommendation	Google is certified to the ISO27001 Standard, which regulates "Cryptography" (ISO 27001:2013, Annex A. 10) Customer data that is uploaded or created is encrypted at rest. We use several layers of encryption to protect customer data; adding redundant data protection and allowing us to select the optimal approach based on application requirements. Google publishes details about encryption and key management options for its Google Cloud Platform and G Suite products. To read more about key management and encryption, please see: https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including development of appropriate encryption measures.
8.2-01		8.2	(1) Protection of personal information within the provider of outsourced storage consignee such as medical record ① Supervising the appropriate consignor For the protection of personal data within the operator who accepts external storage of medical records, etc., refer to Chapter 6 of this Guideline and perform appropriate management.	minimum	N/A
8.2-02			(2) Patient Description of External Storage Implementation A facility entrusting external storage of medical records or the like needs to explain and understand in advance to the patient, through an in-hospital bulletin or the like, the fact that the patient's personal information is sent to and stored in a specific external facility as needed, including its safety and risk. ① Explanation before the start Prior to collecting personal information, including medical conditions, histories, etc., from a patient, explain and understand that external storage is being carried out through in-hospital bulletins, etc. before starting medical care.	minimum	N/A
8.2-03			② Difficult to explain to the patient, but with medical urgency When it is difficult to explain to the principal due to conscious disabilities, cognitive disabilities, and the like, and when there is a medical urgency, the explanation is not necessarily required in advance. When the consciousness is recovered, it is necessary to explain and understand it later.	minimum	N/A
8.2-04			③ It is difficult to explain to the patient, but there is no particular medical urgency. If it is difficult to explain to the individual and understand, including infant cases, and there is no urgency, explain to the parent or parent in principle to obtain understanding. However, when it is difficult to explain, such as when it is suspected that a parent is abused or there is no parent, it is desirable to specify the reason why it is difficult to explain in the medical record or the like.	minimum	N/A
8.3-01		8.3			N/A
8.4-01		8.4	From the viewpoint that medical records are sensitive personal information, when external storage is terminated, certain care must be taken by both the medical institution and the entrusted provider. Medical institutions outsourcing external storage of medical records and the like must periodically examine medical records and the like stored in the outsourced business operator, promptly process medical records and the like for which external storage must be terminated, and audit whether the process has been strictly followed. Also, it is necessary for an operator who accepts external storage to clearly indicate to medical institutions that the stored medical records and the like have been correctly handled and processed in response to a request from the medical institutions and the like. These discarding conventions must be specified in the consignment agreement, etc. before starting external storage. In addition, in preparation for actual disposal, a clearly defined procedure such as a disposal program should be prepared in advance. It must be fully noted that maintaining personal information beyond the agreed period can itself be a problem in protecting personal information that requires these rigorous treatments to both parties. In the case of external storage via a network, the external storage system itself is a kind of database, and should be discarded carefully, including index files. In the case of an electronic medium, the same consideration must be given to backup files. Further, in the case of external storage through a network, since the storage format is an electronic medium by itself, damage at the time of information leakage is expected to be serious in terms of the amount of information. Therefore, sufficient consideration must be given to the protection of personal information, and it must be ensured that the medical institution or the like outsourced for external storage and the entrusted operator can confirm that the information has been reliably discarded. (The guidelines of the MHLW are described in the content of "B. Concepts", but the guidelines of the MIC are described here because they are treated as requirements.)		Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" (ISO 27001:2013,Annex A.11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.

METI "Security Management Guidelines for Information Processing Providers Dealing with Medical Information version2" (Information management GL)				Google Response
Item No		Classification	Guideline	
7.1 Recommended certification and certification for entrusting information processing business related to medical information		Recommendation	(1) As a safety management measure for ISMS when certification is acquired or updated, it is desirable to incorporate a safety management measure presented in this guideline "7 Safety management Requirements for Information Processing Operators Enterprising Medical Information management".	Google is certified to the ISO27001 Standard, which regulates "Compliance with legal and contractual requirements" (ISO 27001:2013, Annex A.18.1). Google provides comprehensive external documentation and whitepapers detailing our security infrastructure and operational model. Google also maintains an internal ISMS and evidence of its effectiveness is provided via ISO 27001 certification.
		Recommendation	(2) Comprehensive ISMS coverage should be provided from the entry point to the exit point of the trusted management medical-information.	Google is certified to the ISO27001 Standard, which regulates "Compliance with legal and contractual requirements" (ISO 27001:2013, Annex A.18.1). Google provides comprehensive external documentation and whitepapers detailing our security infrastructure and operational model. Google also maintains an internal ISMS and evidence of its effectiveness is provided via ISO 27001 certification.
		Recommendation	(3) To ensure that safety management measures are applied properly when medical institutions select service providers, it is recommended to prepare the application declaration for immediate access to the application declaration in response to the request of medical institutions (clarify the management measures specifically considered for handling medical data in the application declaration).	Google is certified to the ISO27001 Standard, which regulates "Compliance with legal and contractual requirements" (ISO 27001:2013, Annex A.18.1). Google provides comprehensive external documentation and whitepapers detailing our security infrastructure and operational model. Google also maintains an internal ISMS and evidence of its effectiveness is provided via ISO 27001 certification.
7.2 Information asset grip	7.2.1 Asset register	Recommendation	(1) When management an asset ledger or the like as a paper document, it is desirable to implement a mechanism that can detect and record an action that violates the restrictions on accesses to the asset ledger or the like.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0
		Recommendation	(2) The following information may be recorded in the asset ledger or the like. ・Reference number ・Name of the asset (name of medical information) ・Type of asset as medical information ・Data Formats and Readability Means ・Location of the asset, whether the asset can be copied, and where the asset can be copied ・Information processing apparatus for storing assets, identification numbers of electronic media, etc. ・Outline of operations of medical institutions handling assets ・management Manager in Information Processing Operators ・Configured access rights and access privileges ・Date and time when the asset occurred, its retention date, and its plan disposal date ・History of processing on assets (storage, delivery, duplicate, disposal, etc.)	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001:2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
		Recommendation	(1) It is desirable to acquire a history of information processing and record the history in an asset ledger or the like.	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001:2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
7.3 Organizational Security grip Measures (System, Operation grip Regulations)				N/A
7.4 Risk assessment in communication routes of medical information				N/A
7.5 Physical Safety Measures	7.5.1 Requirements for the building of medical information processing facilities			N/A
	7.5.2 Requirements for access to medical-information-processing facilities and etc. of access to and from medical-information-processing facilities		(1) When using buildings or areas exclusively used by information processing operators (independent area etc. among proprietary data centers and co-location areas of external data center operators) that can prevent shall access by persons outside the grip of information processing operators	N/A
		Recommendation	(1) As authentication elements used in mechanical authentication devices, it is desirable to combine authentication devices such as hardware tokens or IC cards, storage elements such as personal identification numbers (PIN40), passwords, biometrics, and the like.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0
			(2) When using a server rack etc. installed in a data center operated by an external provider by renting the location	N/A
		Recommendation	(1) As for the locking device of the server rack in which the medical information system is installed, it is desirable to combine an authentication device such as a hardware token or an IC card, a storage element such as a personal identification number (PIN), a password, biometrics information, and the like.	N/A

METI "Security Management Guidelines for Information Processing Providers Dealing with Medical Information version2" (Information management GL)				Google Response
Item No		Classification	Guideline	
			(3) When using server environments operated by external operators (proprietary server, virtual private server etc.)	N/A
				N/A
	7.5.3 Security of the information processing apparatus	Recommendation	(1) Direct interception risks should be considered for cables used for information transmission.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0 Google adheres to all building and facility requirements in the region where its data centers are located.
	7.5.4 Requirements for discarding and reusing information processing devices	Recommendation	(1) Physical destruction measures should be taken by the information processing provider itself. However, when requesting external businesses, the rationale for selection of providers should be given to medical institutions, etc. and approval of outsourcing should be obtained. Receive and store a certificate or the like indicating that information cannot be read due to destructive actions.	Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" ((ISO 27001:2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" ((ISO 27001:2013,Annex A.11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.
	7.5.5. Requirements for taking out the information processing device	Recommendation	(1) The following items can be considered as items included in the taking-out procedure. ・Format of the application form for taking out the machinery (applicant information, approver information, object equipment information, take-out date and time, scheduled return date and time, information on place of taking out, reason of taking out, outline of information stored in the equipment, result of risk evaluation due to taking out, countermeasure in case the equipment is lost or damaged) ・Request approval process ・Return confirmation process, etc.	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001:2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
		Recommendation	(2) The following items may be included in the verification procedure at the time of return. ・Checking machine operation ・Whether or not there is a device that threatens the security of information, such as an eavesdropping device. ・Detection of malicious programs ・Verification of stored information (unauthorized tampering, etc.), etc.	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001:2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
7.6. Technical safety measures	7.6.1.Maintenance of information processing apparatus and software	Recommendation	(1) The change procedure may include the following items. ・Process of notifying the affected parties about the change ・Format of change application form of machinery (applicant information, approver information, object equipment information, change operation start date and time, change operation period, change reason, summary of information stored in equipment, risk evaluation result due to change, countermeasure in case of equipment damage, etc.) ・Request approval process ・Change testing process ・Recovery procedure in case of trouble in the change work ・Change end confirmation process ・The process of monitoring the impact of changes, etc.	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001:2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
	7.6.2. Segregation of development, testing and operation facilities	Recommendation	(1) It is desirable to perform the verification process at both the binary code level and the source code level so that malicious code does not enter into the software.	Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14). Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including managing their system development process.
	7.6.3. Grip measures against malicious codes			N/A
	7.6.4. Requirements for Using a Web Browser	Recommendation	(1) It is desirable to perform setting so that an external application which is not assumed in a business process of a mail client or the like is not activated from a web browser without explicit confirmation.	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001:2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/.
	7.6.5. Grip of services provided by third parties	Recommendation	(1) When external operators perform services, it is desirable to perform operations in situations where authorized personnel of information processing operators or external operators are management.	Google is certified to the ISO27001 Standard, which regulates "Supplier Relationships" (ISO 27001:2013, Annex A.15). Information security oversight and management controls, including vendor security practices are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google directly conducts virtually all data processing activities to provide our services. However, Google may engage some third-party suppliers to provide services related to Cloud Platform, including customer and technical support. Prior to onboarding third-party suppliers, Google conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms.

METI "Security Management Guidelines for Information Processing Providers Dealing with Medical Information version2" (Information management GL)				Google Response
Item No		Classification	Guideline	
	7.6.6. Network security grip	Recommendation	(1) It is desirable to monitor at the network boundary that fraud and suspicious traffic is not flowing from the medical information system from the internal network to the external network.	Google is certified to the ISO27001 Standard, which regulates "Logging and Monitoring" (ISO 27001:2013, Annex A.12.4). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's security monitoring program is focused on information gathered from internal network traffic, employee actions on systems and outside knowledge of vulnerabilities. At many points across our global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections. This analysis is performed using a combination of open-source and commercial tools for traffic capture and parsing. A proprietary correlation system built on top of Google technology also supports this analysis. Network analysis is supplemented by examining system logs to identify unusual behavior, such as attempted access of customer data. Google security engineers place standing search alerts on public data repositories to look for security incidents that might affect the company's infrastructure. They actively review inbound security reports and monitor public mailing lists, blog posts, and wikis. Automated network analysis helps determine when an unknown threat may exist and escalates to Google security staff, and network analysis is supplemented by automated analysis of system logs. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuration of specific monitoring to detect false or unverified data.
	7.6.6. Network security grip	Recommendation	(2) It is desirable that the intrusion detection system itself be set so as not to be subject to hit and unauthorized access (stealth mode), and that the access to the intrusion detection system be appropriately controlled.	Google is certified to the ISO27001 Standard, which regulates "Access to Networks and Network Services" (ISO27001:2013, Annex A.9.1.2), "Network Security Management" (ISO27001:2013, Annex A.13.1). We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately.
	7.6.7. Handling of electronic media	Recommendation	(1) It is preferable that the destruction of the physical electronic medium and the disposal of the destroyed electronic medium be performed by the information processing provider itself. When requesting external expert operators, provide the medical institutions with the rationale for selection of operators for full understanding. Receive and store a certificate or the like indicating that information cannot be read due to destructive actions.	Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" ((ISO 27001:2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" ((ISO 27001:2013,Annex A.11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.
	7.6.7. Handling of electronic media	Recommendation	(2) In the medical information system, it is desirable to delete unnecessary device drivers in order to limit types of electronic media that can be connected to a server or the like. In addition, in order to prevent unauthorized types of devices from being connected, it is preferable that the device drivers cannot be installed or uninstalled by anyone other than the management.	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001:2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
	7.6.7. Handling of electronic media	Recommendation	(3) It is desirable to periodically verify that no unnecessary device driver has been added.	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001:2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
	7.6.8. Security of information exchange			N/A
	7.6.9. Security requirements for medical information systems			N/A
	7.6.10. Security requirements for applications	Recommendation	(1) It is preferable that the safety diagnostic of the application is not performed directly on the provided service, but is performed by preparing a test environment separately.	Google is certified to the ISO27001 Standard, which regulates "Separation of Development, Testing, and Operational Environments" (ISO 27001:2013, Annex A.12.1.4), " and Security in Development and Support Processes" (ISO 27001:2013, Annex A.14.2). Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
	7.6.11. Cryptographic grip Measures	Recommendation	(1) When the cryptographic module uses an external source code or library, it is preferable to use the authenticity of the source code or library after verifying the integrity by electronic signatures or the like from the manufacturer.	N/A
		Recommendation	(2) Cryptographic key generation is preferably implemented in secure environments such as tamper-resistant smart cards, USB tokens devices, etc.	Google is certified to the ISO27001 Standard, which regulates "Cryptography" (ISO 27001:2013, Annex A.10) Google publishes details about encryption and key management options for its Google Cloud Platform and G Suite products. To read more about key management and encryption, please see: https://cloud.google.com/security/encryption-in-transit/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including development of appropriate encryption measures.
		Recommendation	(3) When key escrow is performed in preparation for loss of encryption keys, it is desirable to perform access control so that only legitimate management persons and legitimate processes can access the repositories of encryption keys.	Google is certified to the ISO27001 Standard, which regulates "Cryptography" (ISO 27001:2013, Annex A.10) Google publishes details about encryption and key management options for its Google Cloud Platform and G Suite products. To read more about key management and encryption, please see: https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing cryptographic key management processes.
		Recommendation	(4) In an environment in which an electronic signature applied to a document by a healthcare worker is verified based on an electronic signature method, it is desirable that signature verification can be continued without being affected by the weakening of a cryptographic algorithm.	N/A

METI "Security Management Guidelines for Information Processing Providers Dealing with Medical Information version2" (Information management GL)				Google Response
Item No		Classification	Guideline	
	7.6.12. Log Acquisition and Auditing	Recommendation	(1) It is desirable to periodically verify that the times of all the server devices and the like of the medical information system are synchronized with the standard time provided by the time server and the like.	Google is certified to the ISO27001 Standard, which regulates ""Access Control"" (ISO 27001:2013, Annex A. 9). Google uses a syncronized time-service protocol to ensure all systems have a common time reference. Google makes their NTP protocol public as well for use by customers. https://developers.google.com/time/
		Recommendation	(2) The following items may be recorded in the audit log. ・Worker information (worker ID, permission/prohibition of logon, time and time of use, details of execution work, access source IP address in case of network access) ・File and data access, modification, and delete records (worker ID, accessibility, use time and time, work content, target file or data type) ・Database operation records (worker ID, availability of connection and work, time and time of use, details of execution work, IP address of access source, details of setting change) ・Apply of correction patches (worker ID, changed file) ・Privileged operations (privilege acquirer ID, availability of privilege acquisition, use time and time, execution work content) ・System startup and shutdown events ・Start and end events of the log acquisition function ・Removing an External Device ・Event logs of security devices such as IDSs and IPS ・Logs generated by the operation of services and applications (including logs related to time synchronization)	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A. 9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
		Recommendation	(3) In order to verify the audit log, it is desirable to establish a system capable of sorting by various indexes, such as worker ID, identifier of information (number described in the asset register, etc.), generation time series, access time series, etc., sorting by information type, narrowing down by access time, etc., so that medical information or the like accessed by the worker can be quickly confirmed.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A. 9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
	7.6.13. Access control policy	Recommendation	(1) It is desirable to perform authority management so that information outside the authority given to the worker and operation screens outside the authority are not displayed.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A. 9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
		Recommendation	(2) It is desirable to periodically verify that the prescribed access control policy is appropriately reflected as an access control mechanism such as a file, directory permission, database access, and the like.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A. 9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google periodically reviews logical access to all systems to ensure appropriateness of access. Further, Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
	7.6.14. Grip of operator accesses and operator IDs	Recommendation	(1) It is desirable to periodically confirm that the accessible range of the worker ID permitted to access is as permitted (that is, that it has not been tampered with).	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A. 9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google periodically reviews logical access to all systems to ensure appropriateness of access. Further, Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
		Recommendation	(1) It is preferable to separate the accounts according to the type of privileges and restrict accesses to files and directories.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A. 9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.

METI "Security Management Guidelines for Information Processing Providers Dealing with Medical Information version2" (Information management GL)				Google Response
Item No		Classification	Guideline	
		Recommendation	(2) If possible as a function of the system, it is desirable to limit the range of commands and utilities that can be used with the privilege ID to the minimum range necessary for business, and to prevent unauthorized activities such as tampering and deletion of important commands, utilities, and logs.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A. 9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
		Recommendation	(1) When the worker registers and changes the password for logon to the medical information system, it is desirable to consider a mechanism for ensuring that the predetermined quality is satisfied, introduction of a program or the like for generating a password by a random number, introduction of a system in which the worker is not permitted to set a password having a low quality, and the like.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A. 9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
		Recommendation	(2) As the quality standard of the password, it is considered that the password is sufficiently long (for example, eight characters or more), one or more alphabets, numerals, and symbols are included, and the like.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A. 9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Users are required to authenticate using valid credentials prior to resetting their password. Passwords are managed in accordance with a set of password construction, protection and management guidelines, which enforce the following: a) Minimum length b) Complexity c) History d) Idle time lockout setting Password security requirements are stipulated in the security guidelines and controls (password complexity, expiration, etc.) are built into systems to help ensure that Google password standards are enforced.
		Recommendation	(1) In order to detect that an unauthorized accounts has been used or attempted by the worker, it is desirable to display the date and time of success if the previous logon has succeeded after the logon of the worker, and to display the date and time of failure together with a warning message indicating that there is a possibility that an unauthorized logon attempt has been made by a third party if the previous logon has failed.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A. 9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Users are required to authenticate using valid credentials prior to resetting their password. Passwords are managed in accordance with a set of password construction, protection and management guidelines, which enforce the following: a) Minimum length b) Complexity c) History d) Idle time lockout setting Password security requirements are stipulated in the security guidelines and controls (password complexity, expiration, etc.) are built into systems to help ensure that Google password standards are enforced.
		Recommendation	(2) In order to prevent unauthorized use of the accounts, it is desirable to limit the days of the week and the time zone in which the operator is permitted to log on to the days of the week and the time zone required for the operation.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A. 9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
		Recommendation	(3) When an unauthorized worker or a third party attempts to log on, displaying "password is different" provides a clue to the existence of the worker ID. Therefore, it is preferable to display only a message that does not give special information such as "Authentication failed" or simply redisplay the logon prompt.	Google is certified to the ISO27001 Standard, which regulates "User access management" (ISO 27001:2013, Annex A.9.2). Google native authentication requires a minimum 8 character complex password. Tenants can set the maximum or increase the minimum. A built-in Password Monitor is visible to the end user upon password creation and to the System Administrators of the tenant whom can decide to force a password change on any user that is later detected to have a password that is weak. Google's native authentication has protections in place that would detect a brute force attack and challenge the user to solve a Captcha and would auto lock the account if suspicious activity is detected. The tenant's System Administrators can reset that account for the end user.
		Recommendation	(4) It is recommended that a reasonable approval process be developed when logging on is required outside the specified time for emergency work.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A. 9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.

METI "Security Management Guidelines for Information Processing Providers Dealing with Medical Information version2" (Information management GL)				Google Response
Item No		Classification	Guideline	
		Recommendation	(5) As an authentication element used at the time of logon, it is desirable to combine an authentication device such as a hardware token or an IC card, a storage element such as a personal identification number (PIN), a password, biometrics information, and the like.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A. 9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
	7.6.15. Responsibilities and knowledge of operators			N/A
7.7. Human safety measures		Recommendation	(1) For information processing operators who manipulate medical information, disciplinary procedures should be defined in advance when actions violating the prescribed safety management measures are performed. This can also be included in the service regulations and the like. Make sure that each staff member is informed of and understands the specified disciplinary procedures.	Google is certified to the ISO27001 Standard, which regulates "Information Security Awareness, Education and Training" (ISO 27001:2013, Annex A.7.2.2), Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All Google contractors undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new contractors agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.
7.8. Destruction of information				N/A
7.9. Modification and Maintenance of Medical Information Systems		Recommendation	(1) It is desirable to perform vulnerability detection of developed software at the source code level. When it is impossible to request the provision of source code such as package software, the application is operated instead of the source code level, and the external vulnerability check is performed.	Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14). Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including managing their system development process.
7.10. Business continuity plan for medical information processing	7.10.1. Identification of requirements			N/A
7.10. Business continuity plan for medical information processing	7.10.2. Establishment and review of business continuity plans	Recommendation	(1) The planned business continuity plan should include the following items. ・Prepare Plan ・"emergency" judgment procedure ・Calling related persons and setting up response headquarters ・Degrade actions for equipment and workers and arrangements for alternative facilities ・Actions to switch to alternative facilities, such as backup facilities ・Considerations during the operation of the alternative facilities (e. g., procedures for operating the emergency accounts and considerations for synchronizing health care information to normal systems after recovery) ・Procedures and standards for determining the extent to which the problem has been expanded ・Procedures and Standards for Determining Normal Recovery ・Procedures for checking medical information systems after returning to normal (detection of unauthorized intrusion, information tampering, information corruption, etc.) ・Contact system to administrative authorities, etc.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A. 17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.

METI "Security Management Guidelines for Information Processing Providers Dealing with Medical Information version2" (Security management GL)			Google Response
Section No	Item No	Guideline	
2.1 Recommended certification and certification for entrusting information processing business related to medical information		Organizations entrusted with medical information processing business shall acquire fair third-party certification based on reasonable and objective standards for the purpose of securing medical information.	Google is committed to maintaining a program where independent verification of security, privacy, and compliance controls are regularly reviewed. Google undergoes several independent third party audits to test for data safety, privacy, and security, as noted below: SOC 1 / 2 / 3 (SSAE 18 - formerly SSAE 16 / SAS 70) ISO 27001 ISO 27017 / 27018 PCI - DSS HIPAA For a full list of certificates and compliance materials, please refer to https://cloud.google.com/security/compliance
2.2 Information asset grip	2.2.1 Asset register	(1) Documentation and management of the maintenance of the management ledger for the management of data stored by healthcare institutions, etc.	Google is certified to the ISO27001 Standard, which regulates "Documented Operating Procedures" (ISO27001:2013, Annex A.12.1.1). Google maintains robust internal documentation and maintains an ISMS, per ISO27001 requirements. All documentation in on systems that are replicated and subject to backup. Customers using Google Cloud Platform, retain all rights and responsibilities to configure and manage their environment, including development of operational guidance.
		(2) Record all deposit information in the asset register.	Google is certified to the ISO27001 Standard, which regulates "Documented Operating Procedures" (ISO27001:2013, Annex A.12.1.1). Google maintains robust internal documentation and maintains an ISMS, per ISO27001 requirements. All documentation in on systems that are replicated and subject to backup. Customers using Google Cloud Platform, retain all rights and responsibilities to configure and manage their environment, including development of operational guidance.
		(3) The management should allow for quick access to the assets ledger as needed.	Google is certified to the ISO27001 Standard, which regulates "Documented Operating Procedures" (ISO27001:2013, Annex A.12.1.1). Google maintains robust internal documentation and maintains an ISMS, per ISO27001 requirements. All documentation in on systems that are replicated and subject to backup. Customers using Google Cloud Platform, retain all rights and responsibilities to configure and manage their environment, including development of operational guidance.
		(4) Restrict access to asset ledgers to operators who need to browse and edit.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
		(5) When management an asset ledger or the like as an electronic record, record the actions that violate the restrictions on accesses to the asset ledger or the like.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
	2.2.2 Classification of information	(1) Determine guidelines for classifying information so that information owners and management managers can perform appropriate classifications according to the guidelines.	Google is certified to the ISO27001 Standard, which regulates "Information classification" (ISO 27001:2013, Annex A.8.2). Information security oversight and management controls, including software development controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers can apply their own data-labeling standard to information stored in Google Cloud.
		(2) The owner of the information and the management manager should periodically confirm that the information is classified correctly.	Google is certified to the ISO27001 Standard, which regulates "Information classification" (ISO 27001:2013, Annex A.8.2). Information security oversight and management controls, including software development controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers can apply their own data-labeling standard to information stored in Google Cloud.
		(3) Perform a classification-based risk analysis on the escrowed information.	Google is certified to the ISO27001 Standard, which regulates "Information classification" (ISO 27001:2013, Annex A.8.2). Information security oversight and management controls, including software development controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers can apply their own data-labeling standard to information stored in Google Cloud.
		(4) Depending on the results of risk analyses, implement the management measures required to reduce risk.	Google is certified to the ISO27001 Standard, which regulates "Information classification" (ISO 27001:2013, Annex A.8.2). Information security oversight and management controls, including software development controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers can apply their own data-labeling standard to information stored in Google Cloud.
		(5) The information should be labeled so that the classification can be identified. (Since various methods can be used to label the electronic records, the details and safety of the method to be implemented should be checked and approved by medical institutions.)	Google is certified to the ISO27001 Standard, which regulates "Information classification" (ISO 27001:2013, Annex A.8.2). Information security oversight and management controls, including software development controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers can apply their own data-labeling standard to information stored in Google Cloud.
		(6) Determine the processing method (storage, delivery, browsing, disposal, etc.) corresponding to each label.	Google is certified to the ISO27001 Standard, which regulates "Information classification" (ISO 27001:2013, Annex A.8.2). Information security oversight and management controls, including software development controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers can apply their own data-labeling standard to information stored in Google Cloud.

METI "Security Management Guidelines for Information Processing Providers Dealing with Medical Information version2" (Security management GL)			Google Response
Section No	Item No	Guideline	
2.3 Organizational Security grip Measures (System, Operation grip Regulations)		(1) Establish a policy on safety management of medical information and keep the medical information ready to be submitted in response to requests from medical institutions, etc.	Google is certified to the ISO27001 Standard, which regulates "Information Security Policy" (ISO 27001: 2013, Annex A.5) and Organization of Information Security (ISO27001:2013, Annex A.6). Information security oversight and management controls, including documentation of information security policies are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
		(2) Establish a policy on personal information protection and make it ready for submission in response to requests from medical institutions.	Google is certified to the ISO27001 Standard, which regulates "Information Security Policy" (ISO 27001: 2013, Annex A.5) and Organization of Information Security (ISO27001:2013, Annex A.6). Information security oversight and management controls, including documentation of information security policies are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
		(3) Personal information protection should be performed under the supervision of medical institutions, etc.	Google is certified to the ISO27001 Standard, which regulates "Information Security Policy" (ISO 27001: 2013, Annex A.5) and Organization of Information Security (ISO27001:2013, Annex A.6). Information security oversight and management controls, including documentation of information security policies are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
		(4) Establish procedures and operation management regulations related to safety management of information processing.	Google is certified to the ISO27001 Standard, which regulates "Information Security Policy" (ISO 27001: 2013, Annex A.5) and Organization of Information Security (ISO27001:2013, Annex A.6). Information security oversight and management controls, including documentation of information security policies are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
		(5) The operation management regulations should describe the organizational policy for information security, the management of contracts with external operators such as information processing operators' systems and facilities, medical institutions and cleaning operators, the management methods of hardware/software related to information processing, prevention of risks, response to risks, management of media for storing medical information (storage, transfer, etc.), information security inspection by third parties, and the establishment and response of inquiry windows from medical institutions' management personnel.	Google is certified to the ISO27001 Standard, which regulates "Information Security Policy" (ISO 27001: 2013, Annex A.5) and Organization of Information Security (ISO27001:2013, Annex A.6). Information security oversight and management controls, including documentation of information security policies are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
2.4 .Risk assessment in communication routes of medical information		Treatment of medical information requires high confidentiality. In order to ensure confidentiality, it is necessary to limit the extent of movement of medical information. Recognize routes from the entrance of information to storage locations, storage cabinets with appropriate protective functions and a certain level of strength if electronic media are used, databases with appropriate access management if electro-magnetic recording is used, databases with appropriate access management, file servers, etc., routes for providing medical information to medical institutions, routes for discarding information ultimately, and enumerate threats present on these routes for risk assessment.	Google is certified to the ISO27001 Standard, which regulates "Information security reviews" (ISO 27001: 2013, Annex A.18.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. A formal risk assessment is performed at least annually to determine the likelihood and impact of all identified risks, using qualitative and quantitative methods. The likelihood and impact associated with each risk is determined independently, considering each risk category.
2.5 Physical Safety Measures	2.5.1 Requirements for the building of medical information processing facilities	(1) In order to prevent unauthorized accesses to server equipment or the like in which medical information is stored, locking management and key management of server racks are performed.	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A. 11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers
		(2) In order to prevent unauthorized activities such as interception and theft, the wall, ceiling, and floor sections that divide the room must have a sufficient thickness to provide measures such as constant monitoring with a surveillance camera, storage of image records, and periodic detection of unauthorized devices.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Google adheres to all building and facility requirements in the region where its data centers are located.
		(3) Introducing an intrusion detection device to prevent unauthorized physical intrusion into buildings and rooms.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0 Google adheres to all building and facility requirements in the region where its data centers are located.
		(4) To avoid damage due to natural and human disasters, implement appropriate disaster prevention measures for buildings themselves.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Google adheres to all building and facility requirements in the region where its data centers are located.

METI "Security Management Guidelines for Information Processing Providers Dealing with Medical Information version2" (Security management GL)			Google Response
Section No	Item No	Guideline	
	2.5.2 . Requirements for access to medical-information-processing facilities and etc. of access to and from medical-information-processing facilities	(1) When using buildings or areas exclusively used by information processing operators (independent areas among proprietary data centers and co-location areas of external data center operators) that can prevent access from persons outside the management of information processing operators	N/A
		・In order to restrict access to rooms where medical information is stored by installing medical information systems, a person must be authenticated by installing one or both of a manned reception and a mechanical authentication device to ensure the authenticity of entering and leaving theaters.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored, logged and periodically approved for appropriateness. Google adheres to all building and facility requirements in the region where its data centers are located.
		・When management entrances and exits using mechanical authentication devices without having to accept personnel, use authentication devices using a plurality of factors including one or more biometrics.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0
		・Acquire certification histories for both personnel acceptance and mechanical access management, periodically verify the histories to ensure that there is no suspicious activity (see "2.6.12. Acquiring and Auditing Logs" for the maintenance of the histories).	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0
		・During the job in the area occupied by the information processing business operator, it is mandatory to carry the staff ID card of the information processing business operator in which the facial photograph of the staff is recorded on the ticket from the outside in a visible state, so that it can be identified when a person who is not the staff of the information processing business enters the area.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0
		・The staff member of the information processing service provider must confirm the identity of the person who is not the staff member of the information processing service provider by making a voice or the like when identifying the person in the exclusive area of the information processing service provider.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0

METI "Security Management Guidelines for Information Processing Providers Dealing with Medical Information version2" (Security management GL)			Google Response
Section No	Item No	Guideline	
		・Strict issue and revocation management of staff certificates should be performed when the staff certificate is suspected of being lost or illegally used, such as immediately notifying management personnel, and reliably collecting and discarding staff certificates when staff of an information processing operator leaves the office.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0
		・The time during which stay in the office should be specified according to the work of the staff of the information processing business operator.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored, logged and periodically approved for appropriateness. Employees with access must follow documented policies and procedures for the type of secured areas they are working in.
		・Do not allow personal properties that are not related to the performance of tasks within medical information processing facilities.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0
		(2) When using a data center operated by an external provider by renting the installation location of a server rack or the like	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A. 11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers
		・Ensure that external operators operating data centers are sufficiently secure against physical unauthorized operations by persons outside the management of information processing operators, such as implementing safety management measures equivalent to (1).	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A. 11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers
		・Lock the server rack where the medical information system is installed, and perform reliable key management so that only personnel of the defined information processing service provider can handle the key.	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A. 11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers
		・Record the worker, work start time, work end time, work content, etc. of the work performed by the information processing provider unlocking the server rack in which the medical information system is installed.	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A. 11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers

METI "Security Management Guidelines for Information Processing Providers Dealing with Medical Information version2" (Security management GL)			Google Response
Section No	Item No	Guideline	
		・When an external provider who operates the data center unlocks the server rack and performs work, contact in advance as a rule, and confirm that medical information systems and medical information are not affected.	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A. 11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers
		・In order to prevent other operators who enter the same data center from knowing that the medical information system is a medical information system, information that can identify the type of information handled, the function of the system, etc. should not be made visible from the outside.	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A. 11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers
		(3) When using a server environment (proprietary server, virtual private server, etc.) operated by an external provider	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A. 11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers
		Ensure that external operators operating Ø servers are adequately secure against unauthorized accesses by persons outside the management of information processing operators, such as implementing safety management measures equivalent to (1) and (2).	Google is certified to the ISO27001 Standard, which regulates ""Supplier Relationships"" (ISO 27001: 2013, Annex A.15). Information security oversight and management controls, including vendor security practices are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google directly conducts virtually all data processing activities to provide our services. However, Google may engage some third-party suppliers to provide services related to Cloud Platform, including customer and technical support. Prior to onboarding third-party suppliers, Google conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms.
	2.5.3 Security of the information processing apparatus	(1) To identify unauthorized devices, create and maintain a list of information processing devices used in medical information systems.	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001: 2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
		(2) Do not install unnecessary applications on devices used in medical information systems.	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001: 2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
		(3) Make a layout of equipment in the room so that no unauthorized access to the terminal screen on which medical information or the like is displayed will be viewed. If such a layout is difficult, take measures such as installing a peeping prevention filter on the terminal screen.	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A. 11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers
		(4) Medical information should be saved only in the server device, and should not be saved on the terminal except for temporary storage for display.	Google is certified to the ISO27001 Standard, which regulates "Cryptography" (ISO 27001:2013, Annex A.10) Customer data that is uploaded or created is encrypted at rest. We use several layers of encryption to protect customer data; adding redundant data protection and allowing us to select the optimal approach based on application requirements. Google publishes details about encryption and key management options for its Google Cloud Platform and G Suite products. To read more about key management and encryption, please see: https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including development of appropriate encryption measures.

METI "Security Management Guidelines for Information Processing Providers Dealing with Medical Information version2" (Security management GL)			Google Response
Section No	Item No	Guideline	
		(5) Be careful not to damage the fire equipment in the event of a fire.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers
		(6) To prohibit smoking and eating and drinking in the room where the medical information system is installed.	Google is certified to the ISO27001 Standard, which regulates "Information Security Awareness, Education and Training" (ISO 27001:2013, Annex A.7.2.2), Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All Google contractors undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new contractors agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.
		(7) When placing a fuel-readable object and a liquid in the room where the medical information system is placed, care should be taken not to adversely affect the device, such as maintaining a sufficient distance between the device and providing a dedicated storage facility.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust detection of environmental elements, including heat, fire, smoke and water detection. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, smoke, and water detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
		(8) Maintain and inspect each equipment according to the intervals and specifications specified by the manufacturer or supplier, and replace the equipment if necessary.	Google is certified to the ISO27001 Standard, which regulates "Equipment Maintenance" (ISO 27001:2013, Annex A.11.2.4).
		(9) When a troubleshooting external is performed when a disability or the like is found in the maintenance and inspection, the operation should be performed in an area management to the information processing provider, so that the troubleshooting operation is not carried out to the outside. When it is necessary to carry out an operation to the outside, the electro-magnetic recording in the device should be erased without fail and then taken out. For a device such as a storage device whose information cannot be erased due to a disability, select discard after performing physical destruction instead of repair.	Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" ((ISO 27001:2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" ((ISO 27001:2013,Annex A.11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.
		(10) The following security management measures should be implemented for server racks where medical-information systems are installed. Ii Ensure that you do not fall in the event of an earthquake. There must be sufficient air conditioning equipments to prevent failure by ii thermal, and the server rack must be fully ventilated. Ii A physical locking device with adequate security strength should be provided on the door and the key management should be fully taken into consideration.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google's data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located and maintains facilities that comply with best practices to minimize damage due to natural disasters.
		(11) Set a startup password for an information processing apparatus that can operate reasonably even if the startup password is set. Follow Section 2.6.14, "management of operator accesses and operator IDs" for the qualities and management of passwords to be set.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
		(12) Implement measures such as preparing substitute equipment, making it redundant, and installing backup facilities so that work can be continued even in the event of a failure of an information processing apparatus.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.

METI "Security Management Guidelines for Information Processing Providers Dealing with Medical Information version2" (Security management GL)			Google Response
Section No	Item No	Guideline	
		(13) In order to avoid adverse effects of an unauthorized information processing apparatus being connected to a network, a mechanism for checking consistency with a registered network address, that a malicious program has not been infected, that a vulnerability patch has been applied, and the like before connection should be established and operated.	Google is certified to the ISO27001 Standard, which regulates "Logging and Monitoring" (ISO 27001: 2013, Annex A.12.4). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's security monitoring program is focused on information gathered from internal network traffic, employee actions on systems and outside knowledge of vulnerabilities. At many points across our global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections. This analysis is performed using a combination of open-source and commercial tools for traffic capture and parsing. A proprietary correlation system built on top of Google technology also supports this analysis. Network analysis is supplemented by examining system logs to identify unusual behavior, such as attempted access of customer data. Google security engineers place standing search alerts on public data repositories to look for security incidents that might affect the company's infrastructure. They actively review inbound security reports and monitor public mailing lists, blog posts, and wikis. Automated network analysis helps determine when an unknown threat may exist and escalates to Google security staff, and network analysis is supplemented by automated analysis of system logs. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuration of specific monitoring to detect false or unverified data.
	2.5.4 Requirements for discarding and reusing information processing devices	(1) When a hard disk or the like is reused by another device in the medical information system, erase the data by a reliable method such as erasing the original data by writing the data a plurality of times before reusing the hard disk or the like, and confirm that the information is erased before reuse.	Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" ((ISO 27001:2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" ((ISO 27001:2013,Annex A.11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.
		(2) If passwords for hardware such as BIOS passwords and hard disk passwords for servers are set, delete the passwords.	Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" ((ISO 27001:2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" ((ISO 27001:2013,Annex A.11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.
		(3) When connecting a hard disk to a device, whether it is reused or not, verify that an unauthorized program or the like is not recorded in the device for verification.	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001: 2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/.
		(4) For discarding hard disks, apply erasure of original data by writing data a plurality of times, measures for erasing the original data by strong magnetic, physical destruction measures (such as melting and cutting by high temperature), etc. to prevent reuse and readout of data. Maintain records of outlines of measures performed on the machineries (the format of the target devices, management numbers, workers in charge of work, date and time of work, content of work, etc.) so that they can be submitted promptly in response to requests from healthcare institutions, etc.	Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" ((ISO 27001:2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" ((ISO 27001:2013,Annex A.11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.
	2.5.5. Requirements for taking out the information processing device	(1) Develop appropriate take-out procedures in preparation for taking out the information processing equipment from the room where it is installed and the area management to the information processing operator.	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001: 2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
		(2) Develop appropriate verification procedures to reinstall the removed equipment.	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001: 2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
2.6. Technical safety measures	2.6.1. Maintenance of information processing apparatus and software	(1) Evaluate the effects of changes in the information processing apparatus and software involved in maintenance.	Google is certified to the ISO27001 Standard, which regulates "Equipment Maintenance" (ISO 27001: 2013, Annex A.11.2.4).

METI "Security Management Guidelines for Information Processing Providers Dealing with Medical Information version2" (Security management GL)			Google Response
Section No	Item No	Guideline	
		(2) Consider measures to minimize impact to ensure safe data storage when changes can adversely affect existing operations and equipments.	Google is certified to the ISO27001 Standard, which regulates "Change Management" (ISO27001:2013 Annex A 12.1.2) and "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A. 14). Please see the Google Infrastructure Security Design Overview - https://cloud.google.com/security/security-design/ for more details. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including change management and system development procedures.
		(3) Support the use of previous data formats and protocols for storing and exchanging medical information, if the protocol changes, while the pre-change data formats, medical institutions using the protocol, etc. exist.	Google is certified to the ISO27001 Standards, which regulates "Operational Procedures and Responsibilities" (ISO 27001:2013, Annex A.12.1) and "Network Security" (ISO 27001:2013, Annex A. 13.1). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. System changes that may affect security, availability, processing integrity, or confidentiality are communicated to management and users who will be affected.
		(4) Plan and implement maintenance work of the information processing apparatus and software so as to minimize the stop time of the information processing work.	Google is certified to the ISO27001 Standard, which regulates "Equipment Maintenance" (ISO 27001: 2013, Annex A.11.2.4).
		(5) Develop appropriate procedures for changing information processing apparatuses and software. Maintenance operations should be notified to medical institutions and approved in advance with sufficient room.	Google is certified to the ISO27001 Standard, which regulates "Change Management" (ISO27001:2013 Annex A 12.1.2) and "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A. 14). Please see the Google Infrastructure Security Design Overview - https://cloud.google.com/security/security-design/ for more details. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including change management and system development procedures.
		(6) Perform software integrity checking (tampering detection) periodically to verify that tampering has not been made.	Google is certified to the ISO27001 Standard, which regulates "Logging and Monitoring" (ISO 27001: 2013, Annex A.12.4). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's security monitoring program is focused on information gathered from internal network traffic, employee actions on systems and outside knowledge of vulnerabilities. At many points across our global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections. This analysis is performed using a combination of open-source and commercial tools for traffic capture and parsing. A proprietary correlation system built on top of Google technology also supports this analysis. Network analysis is supplemented by examining system logs to identify unusual behavior, such as attempted access of customer data. Google security engineers place standing search alerts on public data repositories to look for security incidents that might affect the company's infrastructure. They actively review inbound security reports and monitor public mailing lists, blog posts, and wikis. Automated network analysis helps determine when an unknown threat may exist and escalates to Google security staff, and network analysis is supplemented by automated analysis of system logs. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuration of specific monitoring to detect false or unverified data.
		(7) management technical vulnerabilities related to medical-information systems using a ledger, etc.	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001: 2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google. com/about/appsecurity/.
		(8) If potential technical vulnerabilities are identified, perform risk analysis and determine the necessary actions (patch application, configuration change, etc.).	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001: 2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google. com/about/appsecurity/.
		(9) Verify that the patch has not been tampered with and is valid before applying the patch.	Google is certified to the ISO27001 Standard, which regulates "Change Management" (ISO27001:2013 Annex A 12.1.2) and "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A. 14). Please see the Google Infrastructure Security Design Overview - https://cloud.google.com/security/security-design/ for more details. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including change management and system development procedures.
		(10) When re-entrusting maintenance work to external operators, confirm and select that the above requirements are met, and implement the management measure of "2.6.5. management of services provided by third parties". Report selected external operators to medical institutions and obtain agreement.	Google is certified to the ISO27001 Standard, which regulates "Supplier Relationships" (ISO 27001:2013, Annex A.15). Information security oversight and management controls, including vendor security practices are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google directly conducts virtually all data processing activities to provide our services. However, Google may engage some third-party suppliers to provide services related to Cloud Platform, including customer and technical support. Prior to onboarding third-party suppliers, Google conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms.
	2.6.2. Segregation of development, testing and operation facilities	(1) Applications developed by information service providers themselves should be used for information processing. When an application development by an external developer is used, the application should be used after the safety has been fully verified in advance.	"Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14). Please see the Google Infrastructure Security Design Overview - https://cloud.google.com/security/security-design/ for more details. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including system development procedures.
		(2) When developing software, use development information processing facilities that are not directly connected to the operation facilities (hereinafter referred to as "development facilities") to avoid the effects of software failures.	Google is certified to the ISO27001 Standard, which regulates "Separation of Development, Testing, and Operational Environments" (ISO 27001:2013, Annex A.12.1.4), " and Security in Development and Support Processes" (ISO 27001:2013, Annex A.14.2). Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
		(3) In order to prevent malicious code from being mixed at the development facility, the development facility shall follow "2.6.3. Measures to management malicious code" when the development facility has connections to networks (such as the Internet) used by unspecified numbers.	Google is certified to the ISO27001 Standard, which regulates "Separation of Development, Testing, and Operational Environments" (ISO 27001:2013, Annex A.12.1.4), " and Security in Development and Support Processes" (ISO 27001:2013, Annex A.14.2). Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
		(4) In order to avoid the risk of unauthorized software rewriting, tampering prevention and detection measures should be implemented on the software when the developed software is introduced into the operation facility.	Google is certified to the ISO27001 Standard, which regulates "Change Management" (ISO27001:2013 Annex A 12.1.2) and "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A. 14). Please see the Google Infrastructure Security Design Overview - https://cloud.google.com/security/security-design/ for more details. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including change management and system development procedures.

METI "Security Management Guidelines for Information Processing Providers Dealing with Medical Information version2" (Security management GL)			Google Response
Section No	Item No	Guideline	
		(5) Do not copy medical information stored in operation sites to development and testing facilities.	Google is certified to the ISO27001 Standard, which regulates "Separation of Development, Testing, and Operational Environments" (ISO 27001:2013, Annex A.12.1.4), " and Security in Development and Support Processes" (ISO 27001:2013, Annex A.14.2). Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
		(6) Do not use medical information directly as development and testing data. In the case of use, specify data operations such as deleting personal information and replacing some data with random data so that the original data cannot be restored. Indicate to the medical institution that sufficient safety is guaranteed, and use the data after understanding.	Google is certified to the ISO27001 Standard, which regulates "Separation of Development, Testing, and Operational Environments" (ISO 27001:2013, Annex A.12.1.4), " and Security in Development and Support Processes" (ISO 27001:2013, Annex A.14.2). Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
	2.6.3. Grip measures against malicious codes	(1) Collect information on the latest threats, check the extent of malicious code protection software installed, and confirm that there is no leakage of protection. Examples of threats to be addressed include computer viruses (worms), backdoors (Trojan horses), spyware (keyloggers), bot programs (downloaders), etc.	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001:2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/.
		(2) The following settings are made in malicious code protection software. ・Real-time scan (disk read/write, network communication) ・Periodically scan if necessary as a result of risk assessment ・On-demand scan/definition files when writing/reading data to/from electronic media, automatic updating of scan engines, manual updating with adequate frequency, prohibition of setting changes and uninstallation by anyone other than management people	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001:2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/.
		(3) When malicious codes have not been checked for a certain period of time, or when definition files or devices whose scan engines have not been updated have been checked, measures must be taken, such as displaying warning messages to users, notifying management users, and prohibiting or quarantining intra-facility networking.	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001:2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/.
	2.6.4. Requirements for Using a Web Browser	(1) Restrict the servers to which web browsers connect to servers that are required for business.	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001:2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/.
		(2) The web browser must be configured to not allow code to be downloaded and executed from unauthorized sites, such as ActiveX, applets for Java, or Flash (only servers on which management software is executed).	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001:2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/.
		(3) Code downloaded from authorized sites should also be checked against "2.6.3. management measures against malicious code".	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001:2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/.
	2.6.5. Grip of services provided by third parties	(1) Ensure that the safety management measures and service levels of services provided by third parties are adequate.	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
		(2) Periodically verify the implementation, operation, and maintenance of services.	Google is certified to the ISO27001 Standard, which regulates "Information Security Awareness, Education and Training" (ISO 27001:2013, Annex A.7.2.2), Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All Google employees and contractors undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new employees and contractors agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.

METI "Security Management Guidelines for Information Processing Providers Dealing with Medical Information version2" (Security management GL)			Google Response
Section No	Item No	Guideline	
		(3) Make it mandatory to report beforehand and after the implementation of the service, and inspect and confirm the content of the report.	Google is certified to the ISO27001 Standard, which regulates "Supplier Relationships" (ISO 27001:2013, Annex A.15). Information security oversight and management controls, including vendor security practices are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google directly conducts virtually all data processing activities to provide our services. However, Google may engage some third-party suppliers to provide services related to Cloud Platform, including customer and technical support. Prior to onboarding third-party suppliers, Google conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms.
		(4) Personnel carrying out the service must report in advance and do not accept unauthorized personnel when carrying out the service.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0
		(5) If a third party enters the management area while services are in progress, carry an identification card with a facial photograph on the face of the ticket.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0
		(6) Procedures for entering the processing facility according to the implementation of the service shall be the same as the procedures for entering and leaving the staff of the information processing operator.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0
		(7) When changing services, perform appropriate verification that security is still maintained.	Google is certified to the ISO27001 Standard, which regulates "Supplier Relationships" (ISO 27001:2013, Annex A.15). Information security oversight and management controls, including vendor security practices are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google directly conducts virtually all data processing activities to provide our services. However, Google may engage some third-party suppliers to provide services related to Cloud Platform, including customer and technical support. Prior to onboarding third-party suppliers, Google conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms.
		(8) When outsourcing the maintenance and inspection of medical information systems to external operators, implement the management measures in Section 6.8 C of "Guidelines for Safety management of Medical Information Systems, Version 4.1 (Health, Labor and Welfare Department, February 2010)".	N/A
	2.6.6. Network security grip	(1) Provide security gateways (firewalls, routers, etc. installed at network boundaries) to control access to each network interface based on established policies, such as restricting connection destinations and restricting connection times. When a security gateway cannot be installed at a network boundary at the time of using hosting, the same access control shall be performed by individual information processing apparatuses (servers).	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A. 11.2). Google maintains security configurations for its machines and network devices. The configurations are maintained and serve as master copies for comparision against production instances. Deviations are identified and corrected.
		(2) In the security gateway, setting is made so that traffic having an unauthorized IP address cannot pass through (by setting the IP address of a connection device or the like as a private address, and controlling traffic to pass through the security gateway such as a firewall or a VPN device on the basis of the IP address).	Google is certified to the ISO27001 Standard, which regulates "Communications Security" (ISO 27001: 2013, Annex A.13), and "Securing Application Service on Public Networks" ISO 27001:2013, (Annex A. 14.1.2). Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including management of external connections.
		(3) For network devices such as routers, use devices whose safety can be checked.	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A. 11.2). Google maintains security configurations for its machines and network devices. The configurations are maintained and serve as master copies for comparision against production instances. Deviations are identified and corrected.

METI "Security Management Guidelines for Information Processing Providers Dealing with Medical Information version2" (Security management GL)			Google Response
Section No	Item No	Guideline	
		(4) Restrict physical connection of network devices, servers, and terminals to unused network ports.	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A. 11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers
		(5) An intrusion detection system (hereinafter referred to as "IDS") and an intrusion prevention system (hereinafter referred to as "IPS") should be introduced at the boundary of a network connected to medical institutions to detect fraud events on the network or block unauthorized traffic. In cases where machinery cannot be installed at the border of a network, such as when hosting is used, the same control shall be carried out by individual information processing equipment.	Google is certified to the ISO27001 Standard, which regulates "Access to Networks and Network Services" (ISO27001:2013, Annex A.9.1.2), "Network Security Management" (ISO27001:2013, Annex A. 13.1). We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately.
		(6) Updating of signature/detection rules and application of software-security patches should be carried out so that intrusion detection systems can cope with newest hit and unauthorized accesses at all times.	Google is certified to the ISO27001 Standard, which regulates "Access to Networks and Network Services" (ISO27001:2013, Annex A.9.1.2), "Network Security Management" (ISO27001:2013, Annex A. 13.1). We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately.
		(7) When intrusion detection systems detect urgent hit or unauthorized access, they must immediately notify the management personnel by outputting to the monitoring terminal or by e-mail.	Google is certified to the ISO27001 Standard, which regulates "Access to Networks and Network Services" (ISO27001:2013, Annex A.9.1.2), "Network Security Management" (ISO27001:2013, Annex A. 13.1). We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately.
		(8) The record of intrusion detection includes items necessary for post-processing such as unauthorized access.	Google is certified to the ISO27001 Standard, which regulates "Access to Networks and Network Services" (ISO27001:2013, Annex A.9.1.2), "Network Controls" (ISO27001:2013, Annex A.13.1.1). We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately.
		(9) In medical information systems, connection to services on open networks such as the Internet should be limited to the following services. If there are other necessary services, use them after obtaining agreement from medical institutions, etc. ・Use monitoring and remote maintenance of medical information systems from outside ・Download of the latest pattern file of security software ・Downloading security patch files for operating systems and applications ・Access to the time authentication authority at the time of electronic signature, and access to the certificate authority such as a lapse list at the time of electronic signature verification ・Monitoring unauthorized access to security devices such as firewalls, IDS and IPS ・Accessing a Time Distribution Server for Time Synchronization ・Internet services (e.g., access to domain name servers) required to use these services ・Other services necessary for the operation of medical information systems (external authentication server, external medical information database, etc.)	Google is certified to the ISO27001 Standard, which regulates "Communications Security" (ISO 27001: 2013, Annex A.13), and "Securing Application Service on Public Networks" ISO 27001:2013, (Annex A. 14.1.2). Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including management of external connections.
		(10) An appropriate upper limit should be set for the number of simultaneous logon users (OS accounts, etc.) to servers, etc. of medical-information systems.	Google is certified to the ISO27001 Standard, which regulates "Access to Networks and Network Services" (ISO27001:2013, Annex A.9.1.2), "Network Security Management" (ISO27001:2013, Annex A. 13.1). We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately.

METI "Security Management Guidelines for Information Processing Providers Dealing with Medical Information version2" (Security management GL)			Google Response
Section No	Item No	Guideline	
		(11) Record network connection logs (authentication logs and connection logs).	Google is certified to the ISO27001 Standard, which regulates "Access to Networks and Network Services" (ISO27001:2013, Annex A.9.1.2), "Network Security Management" (ISO27001:2013, Annex A. 13.1). We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately.
		(12) Periodically verify the network connection log to verify that no suspicious activity is taking place.	Google is certified to the ISO27001 Standard, which regulates "Access to Networks and Network Services" (ISO27001:2013, Annex A.9.1.2), "Network Security Management" (ISO27001:2013, Annex A. 13.1). We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately.
		(13) Do not use wireless network (including short-range wireless communication such as Bluetooth) LAN in medical information systems that store medical information.	N/A
		(14) Follow the steps below when establishing a VPN connection. l Authentication should be mutually performed between VPN devices at the time of connection. To minimize the risks of interception, replay, etc., use appropriate cryptographic techniques in accordance with Section 2.6.11, "Cryptographic management Measures". l Do not set up a direct path between the private network interface and the Internet interface so that wired traffic does not enter the VPN channel. l Implement measures such as establishing VPN channels for each medical institution to avoid the risk of information confusion between medical institutions when information processing services are entrusted from multiple medical institutions.	Google is certified to the ISO27001 Standard, which regulates "Communications Security" (ISO 27001: 2013, Annex A.13), and "Securing Application Service on Public Networks" ISO 27001:2013, (Annex A. 14.1.2). Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including management of external connections.
	2.6.7. Handling of electronic media	(1) Do not unnecessarily take electronic media out of information processing business facilities. For electronic media such as CDs, DVDs, MOs, etc., use optical media (CD-R, DVDR, etc.) that cannot be additionally written, and reliably dispose of the electronic media by the method shown in (9) after the completion of the data exchanging operation.	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A. 11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers
		(2) When large-capacity electronic media such as MTs, DATs, solid state memory devices, and hard disks are used for data interchange and back-up purposes, strict management should be made. When information is recorded on these electronic media a plurality of times, measures against information leakage such as reliable information erasure should be taken instead of simply overwriting.	Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" ((ISO 27001:2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" ((ISO 27001:2013,Annex A.11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.
		(3) Create and management a register for electronic media. Periodically verify registers and electronic media to verify theft and loss. In the ledger, records should be made regarding the use of electronic media and maintained for a certain period of time after the disposal of electronic media.	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001: 2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
		(4) Cabinets for storing electronic media should be provided with a physically secure locking device with adequate security, and the key management should be carefully considered.	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001: 2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.

METI "Security Management Guidelines for Information Processing Providers Dealing with Medical Information version2" (Security management GL)			Google Response
Section No	Item No	Guideline	
		(5) Storage in a storage environment specified by the manufacturer of the media to minimize the risk of loss of information due to damage to electronic media, etc.	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001: 2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
		(6) Copy the electronic media to other media when the effective use limit period of the electronic media approaches so that the effective use limit period specified by the manufacturer is not exceeded.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing a process to support data file management activities.
		(7) When hard disk drives are used to store data, measures should be taken to prevent RAID-1 or RAID-6 disk failures or more.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
		(8) All electronic media should be labeled to indicate the level of confidentiality of the information being stored.	Google is certified to the ISO27001 Standard, which regulates "Information classification" (ISO 27001: 2013, Annex A.8.2). Information security oversight and management controls, including software development controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers can apply their own data-labeling standard to information stored in Google Cloud.
		(9) When discarding electronic media, apply physical destructive actions (such as high-temperature fusing and cutting) to ensure that the information cannot be read.	Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" ((ISO 27001:2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" ((ISO 27001:2013,Annex A.11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.
	2.6.8. Security of information exchange	(1) The following items should be agreed in advance for information exchange between medical institutions and information processing operators. l Procedures for recording and exchanging information on electronic media l Procedure for exchanging information in document file format via network l Procedure for exchanging information with application input via network ・Method and verification procedure for attaching an electronic signature and a time stamp to information	Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO 27001:2013, Annex A.14). Information security oversight and management controls, including software development controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing a process to support input management activities.
		(2) In the information exchange procedure, the following items should be ensured regardless of the form of transport. ・Identify and record senders and recipients. ・Prevent non-repudiation measures, such as saving shipping slips, giving electronic signatures to document files, and reliably authenticating applications when logging on, so that senders' activities cannot be denied later. ・Agree on the confidentiality level of the information to be exchanged (not lowering the confidentiality level at the recipient). ・Ensure that the exchanged information does not contain malicious code.	Google is certified to the ISO27001 Standard, which regulates "Cryptography" (ISO 27001:2013, Annex A.10) Encryption is used to protect user authentication and administrator sessions transmitted over the Internet. Remote access to Google corporate machines requires a Google issued digital certificate installed on the connecting device and two-factor authentication. Google publishes details about encryption and key management options for its Google Cloud Platform and G Suite products. To read more about key management and encryption, please see: https://cloud.google.com/security/encryption-at-rest/ https://cloud.google.com/security/encryption-in-transit/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including development of appropriate encryption measures.
		(3) The following measures should be taken when physically conveying information. ・Choose a reliable carrier based on standards agreed upon by medical institutions, etc. ・Identification of operators at the time of delivery should be checked at both the sender and receiver to prevent third-party spoofing. ・In order to prevent electronic media from being picked up by a distributor or the like, the number and type of electronic media to be exchanged must be exchanged in advance to confirm that there is no loss at the time of receipt. ・To prevent information from being extracted from an electronic medium by a distributor or the like, a container or the like that can detect unauthorized opening should be used. ・When electronic media is sent or received, it must be sent directly to the carrier and not through a third party. ・When exchanging information via electronic media, the materials in the electronic media should be encrypted if there are risks in the safety management during the transfer of the data.	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A. 11.2). Google’s focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers

METI "Security Management Guidelines for Information Processing Providers Dealing with Medical Information version2" (Security management GL)			Google Response
Section No	Item No	Guideline	
		(4) The following measures should be taken when electronically transferring datum. ・The sender and the recipients must authenticate each other electronically to verify the validity of the other party. Although the authentication method varies depending on the connection mode and the application used for transfer, it is desirable to authenticate the equipments and the users. ・The transmission and reception paths should be protected from the risk of interception in an appropriate way. ・Measures should be taken to verify that the received information is not damaged or tampered on the way. ・When transmission and reception fail, retransmission and reception should be attempted with a predefined number of times as an upper limit. When the upper limit is reached, all communication between the sender and receiver should be stopped, and work such as specifying a disability should be performed.	Google is certified to the ISO27001 Standard, which regulates "Cryptography" (ISO 27001:2013, Annex A.10) Encryption is used to protect user authentication and administrator sessions transmitted over the Internet. Remote access to Google corporate machines requires a Google issued digital certificate installed on the connecting device and two-factor authentication. Google publishes details about encryption and key management options for its Google Cloud Platform and G Suite products. To read more about key management and encryption, please see: https://cloud.google.com/security/encryption-at-rest/ https://cloud.google.com/security/encryption-in-transit/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including development of appropriate encryption measures.
	2.6.9. Security requirements for medical information systems	(1) Do not place development code or development tools such as compilers on the operation system to avoid confusion of the operation system.	Google is certified to the ISO27001 Standard, which regulates "Separation of Development, Testing, and Operational Environments" (ISO 27001:2013, Annex A.12.1.4), " and Security in Development and Support Processes" (ISO 27001:2013, Annex A.14.2). Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
		(2) Do not place files or the like unnecessary for information processing on the operation system.	Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO 27001:2013, Annex A.14). Information security oversight and management controls, including software development controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing a process to support program file management activities.
		(3) Ensure that the software and operating system software for business use are fully tested before installation.	Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14). Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including managing their system development process.
		(4) Acquire logs necessary for auditing for updating library programs related to the operation system.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google has implemented monitoring tools to detect and report application vulnerabilities. Google also maintains user access logs for privileged access and for access to user data. Logical access to audit logs is restricted to authorized personnel.
		(5) Acquire logs for duplicate and use of system operation information (system and service configuration files, etc.) as audit trails.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
	2.6.10. Security requirements for applications	(1) Regarding the applications to be provided, safety diagnostics including specific vulnerability detection by application type should be performed periodically, and measures should be taken based on the results. Introduce mechanisms to verify the integrity of data when sending and receiving data to and from healthcare institutions.	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" ISO 27001: 2013, (Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/. Within Google, members of the information security team review security plans for all networks, systems and services. They provide project-specific consulting services to Google's product and engineering teams. They monitor for suspicious activity on Google's networks, address information security threats, perform routine security evaluations and audits, and engage outside experts to conduct regular security assessments. We specifically built a full-time team, known as Project Zero, that aims to prevent targeted attacks by reporting bugs to software vendors and filing them in an external database.
		(2) For applications and third-party software (libraries, server processes, etc.) to be used for application operation, refer to the latest vulnerability information to be disclosed and take prompt measures.	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001: 2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/.
		(3) When registering, editing, and deleting information in an application, design and implementation should be performed so as to log on in order to identify the user and confirm the authority.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.

METI "Security Management Guidelines for Information Processing Providers Dealing with Medical Information version2" (Security management GL)			Google Response
Section No	Item No	Guideline	
		(4) Information (password for ID/password authentication) for authenticating the worker at the medical operator side by the application should be stored as an output value of a hash function having sufficient strength, or should be encrypted and stored.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Users are required to authenticate using valid credentials prior to resetting their password. Passwords are managed in accordance with a set of password construction, protection and management guidelines, which enforce the following: a) Minimum length b) Complexity c) History d) Idle time lockout setting Password security requirements are stipulated in the security guidelines and controls (password complexity, expiration, etc.) are built into systems to help ensure that Google password standards are enforced.
		(5) For information manipulation by applications, access management corresponding to functional authorities of medical institutions should be enabled, and information creation, editing, deletion, etc. should be prevented by those who do not have legitimate access authorities.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
	2.6.11. Cryptographic grip Measures	(1) Use cryptographic algorithms with sufficient security. Use e-Government Recommended Cryptography Lists as selection criteria.	Google is certified to the ISO27001 Standard, which regulates "Cryptography" (ISO 27001:2013, Annex A.10) Customer data that is uploaded or created is encrypted at rest. We use several layers of encryption to protect customer data; adding redundant data protection and allowing us to select the optimal approach based on application requirements. Google publishes details about encryption and key management options for its Google Cloud Platform and G Suite products. To read more about key management and encryption, please see: https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including development of appropriate encryption measures.
		(2) Develop countermeasures against leakage of encryption keys.	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" ISO 27001:2013, (Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/. Within Google, members of the information security team review security plans for all networks, systems and services. They provide project-specific consulting services to Google's product and engineering teams. They monitor for suspicious activity on Google's networks, address information security threats, perform routine security evaluations and audits, and engage outside experts to conduct regular security assessments. We specifically built a full-time team, known as Project Zero, that aims to prevent targeted attacks by reporting bugs to software vendors and filing them in an external database.
		(3) When electronic certificates are used for electronic signatures, network connections, etc., electronic certificates must be issued by trusted organizations.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Google uses certificates and ACLs to achieve authentication integrity.
		(4) In preparation for compromise of cryptographic algorithms and cryptographic keys, care should be taken to enable switching of cryptographic algorithms.	Google is certified to the ISO27001 Standard, which regulates "Cryptography" (ISO 27001:2013, Annex A.10) Customer data that is uploaded or created is encrypted at rest. We use several layers of encryption to protect customer data; adding redundant data protection and allowing us to select the optimal approach based on application requirements. Google publishes details about encryption and key management options for its Google Cloud Platform and G Suite products. To read more about key management and encryption, please see: https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including development of appropriate encryption measures.
		(5) The public key certificate of the root certification authority for verifying data received from medical institutions should be obtained through a secure route and compared with fingerprints obtained through another route to verify the authenticity.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Google uses certificates and ACLs to achieve authentication integrity.
	2.6.12. Log Acquisition and Auditing	(1) Create and management audit logs that record activities of workers, events occurring in devices, system failures, and system usage.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google has implemented monitoring tools to detect and report application vulnerabilities. Google also maintains user access logs for privileged access and for access to user data. Logical access to audit logs is restricted to authorized personnel.
		(2) Periodically verify audit logs to detect unauthorized activities, system abnormalities, etc.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google maintains a Data Security Policy that governs access to data and mechanisms to prevent and detect unauthorized access.
		(3) In order to accurately verify the cause of accident, etc. by using the log, the time of all the server devices, etc. of the medical information system should be synchronized with the standard time provided by the time server, etc.	Google is certified to the ISO27001 Standard, which regulates """"Access Control"""" (ISO 27001:2013, Annex A.9). Google uses a syncronized time-service protocol to ensure all systems have a common time reference. Google makes their NTP protocol public as well for use by customers. https://developers.google.com/time/

METI "Security Management Guidelines for Information Processing Providers Dealing with Medical Information version2" (Security management GL)			Google Response
Section No	Item No	Guideline	
		(4) A trusted authority should be used as the time provider for synchronization with the standard time.	Google is certified to the ISO27001 Standard, which regulates ""Access Control"" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google has implemented monitoring tools to detect and report application vulnerabilities. Google also maintains user access logs for privileged access and for access to user data. Logical access to audit logs is restricted to authorized personnel.
		(5) Apply the following management measures to properly protect logs from unauthorized accesses. ・Restrict operator and operation to access log data. ・In order to avoid a situation in which a log cannot be acquired due to an excess of the capacity, the storage capacity of the log server should be constantly monitored, and measures should be taken such as writing to an electronic medium and increasing the capacity. ・Measures to detect and prevent unauthorized tampering and delete of log data.	Google is certified to the ISO27001 Standard, which regulates ""Access Control"" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google maintains a Data Security Policy that governs access to data and mechanisms to prevent and detect unauthorized access.
	2.6.13. Access control policy	(1) To organize security requirements of each information processing apparatus used for information processing.	Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14). Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including managing their system development process.
		(2) Organize the security requirements of each software used for information processing.	Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14). Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including managing their system development process.
		(3) Provide access authority registration requests, change applications, abandonment applications, and approval and periodic verification processes for them.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
		(4) To appropriately group information and control access to groups of information so as to minimize workers having authority to access each information.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
		(5) Establish the minimum necessary access privileges in consideration of the content of work, and set the privileges in the application and the operation system.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
	2.6.14. Grip of operator accesses and operator IDs	(1) The worker is identified by a unique worker ID on the information processing apparatus.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.

METI "Security Management Guidelines for Information Processing Providers Dealing with Medical Information version2" (Security management GL)			Google Response
Section No	Item No	Guideline	
		(2) Introduce a mechanism to eliminate duplication with existing IDs when issuing worker IDs.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
		(3) The use of group IDs for sharing by a plurality of workers shall not be performed in principle, but a mechanism shall be used in which the group ID is changed after logging on with the worker ID so that the operator of the operation can be identified on the log if necessary for business.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google periodically reviews logical access to all systems to ensure appropriateness of access. Further, Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
		(4) Issuance of operator IDs should be limited to the minimum number of people required for management of medical-information systems.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
		(5) When a worker changes or leaves the office, the worker ID must be stopped immediately.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google periodically reviews logical access to all systems to ensure appropriateness of access. Further, Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
		(6) The worker ID used in the past should not be reused in order to reliably specify the worker when the monitoring log is inspected.	Google is certified to the ISO27001 Standard, which regulates ""Access Control"" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google periodically reviews logical access to all systems to ensure appropriateness of access. Further, Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
		(7) Check periodically that no unnecessary worker IDs remain.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google periodically reviews logical access to all systems to ensure appropriateness of access. Further, Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
		(8) Issuance of privilege IDs should be limited to the minimum required.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.

METI "Security Management Guidelines for Information Processing Providers Dealing with Medical Information version2" (Security management GL)			Google Response
Section No	Item No	Guideline	
		(9) Restrict worker IDs that can be promoted to privileged users.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
		(10) When using privileges, record the details of the operation.	Google is certified to the ISO27001 Standard, which regulates ""Access Control"" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google has implemented monitoring tools to detect and report application vulnerabilities. Google also maintains user access logs for privileged access and for access to user data. Logical access to audit logs is restricted to authorized personnel.
		(11) Disable direct logon with privileged IDs from other than management terminals.	Google is certified to the ISO27001 Standard, which regulates ""Access Control"" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
		(12) Delete or change passwords for accounts that are not required, such as the default accounts and maintenance accounts set by the manufacturer, prior to using the information processing equipment and software.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google periodically reviews logical access to all systems to ensure appropriateness of access. Further, Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
		(13) Store information in a form that does not allow easy restoration of passwords, such as storing passwords with hash values, encryption, etc. for logon to medical information systems.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Users are required to authenticate using valid credentials prior to resetting their password. Passwords are managed in accordance with a set of password construction, protection and management guidelines, which enforce the following: a) Minimum length b) Complexity c) History d) Idle time lockout setting Password security requirements are stipulated in the security guidelines and controls (password complexity, expiration, etc.) are built into systems to help ensure that Google password standards are enforced.
		(14) Set the expiration date for the password for logging on to the medical information system and force the operator to change the password periodically.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Users are required to authenticate using valid credentials prior to resetting their password. Passwords are managed in accordance with a set of password construction, protection and management guidelines, which enforce the following: a) Minimum length b) Complexity c) History d) Idle time lockout setting Password security requirements are stipulated in the security guidelines and controls (password complexity, expiration, etc.) are built into systems to help ensure that Google password standards are enforced.
		(15) A historical management of passwords for logging on to medical-information systems should be introduced so that passwords that are identical to passwords of a certain number of generations cannot be reset when they are changed.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Users are required to authenticate using valid credentials prior to resetting their password. Passwords are managed in accordance with a set of password construction, protection and management guidelines, which enforce the following: a) Minimum length b) Complexity c) History d) Idle time lockout setting Password security requirements are stipulated in the security guidelines and controls (password complexity, expiration, etc.) are built into systems to help ensure that Google password standards are enforced.
		(16) A mechanism shall be used in which the input of the password before the change is requested when the password is changed, and the password change is not accepted for a certain period of time when the input of the password before the change fails a certain number of times or more.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Users are required to authenticate using valid credentials prior to resetting their password. Passwords are managed in accordance with a set of password construction, protection and management guidelines, which enforce the following: a) Minimum length b) Complexity c) History d) Idle time lockout setting Password security requirements are stipulated in the security guidelines and controls (password complexity, expiration, etc.) are built into systems to help ensure that Google password standards are enforced.

METI "Security Management Guidelines for Information Processing Providers Dealing with Medical Information version2" (Security management GL)			Google Response
Section No	Item No	Guideline	
		(17) When issuing a password, issue a password for logon to a provisional medical information system generated from a random number, and take measures against password theft risk by forcibly changing the password at the time of first logon.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
		(18) Create standards for the quality to be met by passwords and ensure that all passwords meet the quality standards.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
		(19) Ensure workers do not use the automatic logon function to store passwords in the system.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
		(20) To preserve the authenticity and integrity of files storing password-related data, security measures should be adopted, such as obtaining and verifying hash values of files, giving and verifying digital signatures to files, and encrypting and storing files. Also, restrict access by ordinary workers.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Users are required to authenticate using valid credentials prior to resetting their password. Passwords are managed in accordance with a set of password construction, protection and management guidelines, which enforce the following: a) Minimum length b) Complexity c) History d) Idle time lockout setting Password security requirements are stipulated in the security guidelines and controls (password complexity, expiration, etc.) are built into systems to help ensure that Google password standards are enforced.
		(21) To reduce the risk of hijacking a terminal or a session, a session in which a certain interruption time has elapsed after the operator logs on should be blocked or forcibly logged off.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Google maintains a Data Security Policy that governs access to data and mechanisms to prevent and detect unauthorized access.
		(22) Set a certain refractory time for re-entry when password entry is unsuccessful. A mechanism that does not accept re-entry for a certain period of time should be adopted when logon fails continuously. If this happens, a mechanism should be introduced to send alert messages to the systems management.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Users are required to authenticate using valid credentials prior to resetting their password. Passwords are managed in accordance with a set of password construction, protection and management guidelines, which enforce the following: a) Minimum length b) Complexity c) History d) Idle time lockout setting Password security requirements are stipulated in the security guidelines and controls (password complexity, expiration, etc.) are built into systems to help ensure that Google password standards are enforced.
	2.6.15. Responsibilities and knowledge of operators	(1) Operators should stealthy their passwords and keep them in a safe place to protect them from access, modification, or disposal by others if they need to keep them in a safe place.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
		(2) Change password or disable accounts immediately and notify management personnel when unauthorized access to systems is suspected or the password may be known to third parties.	Google is certified to the ISO27001 Standard, which regulates "Access to Networks and Network Services" (ISO27001:2013, Annex A.9.1.2), "Network Controls" (ISO27001:2013, Annex A.13.1.1). We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately.

METI "Security Management Guidelines for Information Processing Providers Dealing with Medical Information version2" (Security management GL)			Google Response
Section No	Item No	Guideline	
		(3) Locking or logging off the terminal when leaving or not using the terminal to prevent the use of a third party in advance.	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A. 11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers
2.7. Human safety measures		(1) For all information processing operator personnel who may manipulate medical information, the stealthy retention contract must be signed at the time of employment contract or as a condition for the task of handling medical information. Telecommunications employees should be selected and dispatched on the assumption that stealthy must be retained and continuous information-security education must be imposed.	Google is certified to the ISO27001 Standard, which regulates ""Terms and Conditions of Employment"" (ISO 27001:2013, Annex A.7.1.2), Hiring practices controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google performs background checks on new hires as permitted by local laws
		(2) Educate all information processing operators who may operate medical information about information security and select only those who obtain a certain level of understanding. For dispatch employees, ask the dispatcher to select and dispatch personnel who have or can have a certain level of knowledge and understanding of information security. After acceptance, provide training equivalent to regular personnel. This education should be conducted periodically according to new threats and changes in information security technology.	Google is certified to the ISO27001 Standard, which regulates "Information Security Awareness, Education and Training" (ISO 27001:2013, Annex A.7.2.2), Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All Google contractors undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new contractors agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.
		(3) In the event of suspicion of violations of safety management measures by staff of information processing operators, the right to access medical information must be immediately stopped to verify that no action such as tampering or destruction has been performed.	Google is certified to the ISO27001 Standard, which regulates "Access to Networks and Network Services" (ISO27001:2013, Annex A.9.1.2), "Network Controls" (ISO27001:2013, Annex A.13.1.1). We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately.
		(4) When staff of an information processing business operator who operates medical information leaves the office, return all of the lent information assets, and prescribe a ledger and return confirmation procedure to confirm that the return is complete. It is also necessary to sign an agreement that states that medical information learned from work should be management as stealthy after retirement. For dispatch employees, request a signature on the same agreement at the time of cancellation of the dispatch contract.	Google is certified to the ISO27001 Standard, which regulates ""Terms and Conditions of Employment"" (ISO 27001:2013, Annex A.7.1.2), Hiring practices controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google performs background checks on new hires as permitted by local laws
		(5) In contract for commissioning with healthcare institutions, provision must be made for the confidential management of deposit information, such as the agreement to retain stealthy with staff of information processing operators, the provision of information security education, and the disciplinary regulations against the regulations when deposit information is handled illegally.	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
2.8. Destruction of information		(1) Refer to "2.6.7. Handling of electronic media" for disposal of CD-R, etc.	N/A
		(2) Refer to "2.5.4. Requirements for Discard and Reuse of Information Processing Devices" for discard of hard disks and the like.	N/A
		(3) Information Processing Operators shall submit records of information destruction in accordance with the Guidelines on Safety management of Medical Information Systems.	Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" (ISO 27001:2013,Annex A.11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.
2.9. Modification and Maintenance of Medical Information Systems		When upgrading the operating system and applying security patches, evaluate the impact on medical information systems and check the test results before performing the upgrade.	Google is certified to the ISO27001 Standard, which regulates "Separation of Development, Testing, and Operational Environments" (ISO 27001:2013, Annex A.12.1.4), " and Security in Development and Support Processes" (ISO 27001:2013, Annex A.14.2). Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
2.10. Business continuity plan for medical information processing	2.10.1. Identification of requirements	(1) Identify business processes related to medical information processing (including workers for carrying out processes), information processing facilities, etc.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.

METI "Security Management Guidelines for Information Processing Providers Dealing with Medical Information version2" (Security management GL)			Google Response
Section No	Item No	Guideline	
		(2) Evaluate interrelationships between business processes.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
		(3) Clarify the priorities of business processes to continue business.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
		(4) Identify the impact of hardware and software failures on medical information systems on business processes.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
		(5) Identify the effects and interactions of hardware and software faults occurring in medical information systems on other hardware and software, and identify the hardware and software with the greatest impact.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
		(6) Assess the magnitude of the impact of hardware and software, and consider measures such as making the system part redundant, or allowing the system part to be outputted to external files in a format that ensures readability (format such as PDF, JPEG, or PNG) so that information can be browsed using general-purpose browsers, etc. in case the system becomes unable to be browsed due to a disability.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
		(7) If necessary for continuing the information processing services provided to medical institutions, etc., an alternative information processing facility for continuing the information processing services, such as a backup facility for medical information to be entrusted, shall be established, and physical safety measures presented in this guideline shall be provided for those facilities.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions.

METI "Security Management Guidelines for Information Processing Providers Dealing with Medical Information version2" (Security management GL)			Google Response
Section No	Item No	Guideline	
	2.10.2. Establishment and review of business continuity plans	(1) Establish a business continuity plan for medical information processing based on the priorities of business processes and medical information systems in the service provision of medical information systems.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
		(2) Review the planned business continuity plan in an appropriate manner, including simulated testing.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
		(3) Periodically review the business continuity plan.	Google is certified to the ISO27001 Standard, which regulates ""Redundancies"" (ISO27001:2013, Annex A.17.2) and ""Backup"" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.

MIC "Security Management Guidelines for Cloud Service Providers Handling Medical Information version1"			Google Response (EN)
Item No		Guideline	
3.2.1	(A)	① Establish a responsibility person responsible for grip the provision of services. ② Establish a responsibility person (system grip person) who is responsible for the grip of the information system and who has adequate technical skills and experiences in this information system. ③ Establish a responsible person for supervising operations related to the operation of information systems related to the provision of services. ④ Develop rules for designation and dismissal of responsible persons listed in (1) to (3).	Google is certified to the ISO27001 Standard, which regulates "Information Security Policy" (ISO 27001:2013, Annex A.5) and Organization of Information Security (ISO27001:2013, Annex A.6). Information security oversight and management controls, including documentation of information security policies are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
3.2.1	(B)1	① Include information on services and confidentiality obligations on commissioned information in service provision contracts. The contract includes the fact that a penalty is imposed on a cloud service provider that violates the confidentiality obligation, and the contents related to the supervision by medical institutions and the like on the treatment of the consigned information.	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.2.1	(B)2	① Clear that the contract for providing services complies with the content of the operation grip regulations and other latest related laws and regulations set forth in the following section (c) 1. and that safety grip actions should be implemented.	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.2.1	(B)3	① Include compliance with this guideline as well as the MHLW and METI guidelines in the service provision agreement. ② When presenting to medical institutions the status of compliance with the guidelines shown in (1) as concrete as possible (e.g., providing information compliant with the guidelines for disclosing information on safety and reliability of ASPs and SaaS (Medical Information Handling Services) ("March 31, 2017"), which are established by the MIC, etc.)	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.2.1	(C)1	① Management clarifies its personal data policies, privacy policies, etc. ② The guidelines for (1) include the implementation of safety grip actions specified in the guidelines of the personal data Protection Act and the personal data Protection Committee. ③ The guidelines for (1) include the fact that even information not covered by the personal data protection law (information related to dead persons, etc.) is handled in accordance with the operation of the personal data protection law due to the special nature of medical information. ④ Develop information security policies, including policies related to information security, including operational grip regulations, etc. ⑤ Establish and document an organizational system that ensures compliance with information security policies. ⑥ Basic policy security policies in organizational efforts related to information security should be agreed with medical institutions based on the service specification conformance disclosure document.	Google is certified to the ISO27001 Standard, which regulates "Information Security Policy" (ISO 27001:2013, Annex A.5) and Organization of Information Security (ISO27001:2013, Annex A.6). Information security oversight and management controls, including documentation of information security policies are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
3.2.1	(C)2	① Clarify the system for providing services, including emergency response. ② Based on the Service Specification Compliance Disclosure Form, agree with medical institutions to disclose information related to systems related to the provision of services (including information related to systems by re-commissioning).	Google is certified to the ISO27001 Standard, which regulates "Information Security Policy" (ISO 27001:2013, Annex A.5) and Organization of Information Security (ISO27001:2013, Annex A.6). Information security oversight and management controls, including documentation of information security policies are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
3.2.1	(C)3	① Create important documents, such as basic policies on information security and operation grip regulations, and formulate regulations on grip, and grip the documents based on these. ② Appropriate documentation of the operation of services and resource grip shall be provided for grip as security-related information. ③ With respect to document grip such as manuals related to the operation of the service, etc., the extent of disclosure and conditions required for disclosure are agreed with the medical institution, etc. based on the service specifications conformance disclosure document. ④ Agree with medical institutions, etc. to provide documentations related to the grip of medical information, based on the service-specification conformance disclosures.	Google is certified to the ISO27001 Standard, which regulates "Documented Operating Procedures" (ISO27001:2013, Annex A.12.1.1). Google maintains robust internal documentation and maintains an ISMS, per ISO27001 requirements. All documentation in on systems that are replicated and subject to backup. Customers using Google Cloud Platform, retain all rights and responsibilities to configure and manage their environment, including development of operational guidance.
3.2.1	(C)4	① Analyze the risk related to the service and decide to take necessary measures. ② Based on the Service Specification Adaptation Disclosure Form, agree with medical institutions on the results of risk analysis related to services, countermeasures and responses to incidents, etc.	Google is certified to the ISO27001 Standard, which regulates "Information security reviews" (ISO 27001:2013, Annex A.18.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. A formal risk assessment is performed at least annually to determine the likelihood and impact of all identified risks, using qualitative and quantitative methods. The likelihood and impact associated with each risk is determined independently, considering each risk category.
3.2.1	(C)5	① Document of grip methods of equipments, etc. ② Determine whether or not to confirm the location of the equipment, etc. by ledger grip, etc. ③ Agree with medical institutions etc. on the company's management regulations regarding grip of equipment etc. based on the service-specification conformance disclosure document.	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001:2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
3.2.1	(C)6	① Develop operational rules for grip of media on which personal data is recorded. ② Agree with medical institutions for operational regulations related to grip of media on which personal data is recorded, based on the service-specification conformance disclosures.	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A.11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers
3.2.1	(C)7	① Regarding the provision of information by cloud service providers when explanations and consent are obtained from medical institutions and the like to the patient, agree with medical institutions and the like on the extent of the provision and roles played by the cloud service providers based on the service specification adaptation disclosure document.	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/

MIC "Security Management Guidelines for Cloud Service Providers Handling Medical Information version1"			Google Response (EN)
Item No		Guideline	
3.2.1	(C)8	① Cluster the policies and content of audits on information systems, organizational systems, operations, etc. that provide services. ② In the case of using cloud responses provided by third parties, clarify the policies and content of auditing or alternatives to the cloud services. ③ Record auditing practices and clarify how to preserve and grip such records. ④ Consistent with the Service Specification Adaptation Disclosure Form with medical institutions for information system audits, etc. to be conducted in-house. ⑤ The extent and conditions of audit records disclosed to medical institutions, etc. are agreed with medical institutions, etc. on the basis of the service specification conformance disclosure document.	Google is certified to the ISO27001 Standard, which regulates "Information Systems Audit Considerations" (ISO 27001:2013, Annex A.12.7), Information security oversight and management controls, including vendor security practices are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google has an established Internal Audit function responsible for evaluating management's compliance with Google's identity management, source code management and infrastructure controls.
3.2.1	(C)9	① Establish a contact point for inquiries from medical institutions and other grip personnel. Agree with medical institutions etc. on the time zone of reception based on the service specification conformance disclosure document. ② Even when a service is provided using a cloud service provided by a third party contracted by the company, inquiry desks from medical institutions and the like are unified.	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.2.1	(D)1	① Develop access grip rules that include the gathering and storage of records on access rights, accounts grip, authentication, and access to information systems by cloud service providers, and periodic reviews on the operational status of the access grip. ② Develop access grip rules that include preservation of access records related to the provision of services (including external access, user access, etc.), and periodic reviews and improvements of records.	Google is certified to the ISO27001 Standard, which regulates "Information Security Policy" (ISO 27001:2013, Annex A.5) and Organization of Information Security (ISO27001:2013, Annex A.6). Information security oversight and management controls, including documentation of information security policies are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
3.2.1	(D)2	① Include the following in the contract regarding the treatment of medical information. ・Grip the personal data as appropriate, distinguishing it from other types of information. ・Clarify that medical information should be handled in accordance with personal data, even if medical information is related to dead persons.	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.2.2	(A)1	① Locking grip shall be performed for security boundaries such as installation locations of equipments, media, etc. used for services. ② Locking grip shall be performed for racks, etc. that store servers, etc. to be used for services. ③ Locking grip shall be carried out for cabinets and the like that store media and the like to be used for services.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0
3.2.2	(A)2	① Restrict installation of equipments and media for services so that only authorized persons can enter and leave. ② Grip of access to equipment and media for services (including reviewing access records) is performed periodically. ③ Grip to enter and leave security boundaries, such as where equipments and media are installed, should be controlled by individual identification systems to identify people who enter and leave the service. When it is difficult to do so, measures are taken to identify the person entering or leaving, for example, changing the personal identification number or the like necessary for entering or leaving on a weekly basis. ④ In order to find out whether or not an unknown person enters or leaves the installation location of the equipment or media used for the service, the user is obliged to wear a name bid or the like. ⑤ Restrict the bringing in of personal properties irrelevant to the performance of services to the installation locations of equipments and media used for services. ⑥ Information that allows identification of the type of information handled, the function of the system, and the like should not be seen from the outside of the storage location (including rack and storage) of the equipment and media used for the service. ⑦ Items (1) to (6) shall be stipulated in the Operational grip Rules, etc.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0
3.2.2	(A)3	① The facilities for physically preserving the equipment and media used for the service shall be installed in buildings that have functions and structures that can withstand disasters (earthquakes, water damage, thunder, fires, etc. and associated power outages) and that take measures against disaster failures (crippling, etc.). ② Architectures in which facilities are installed shall be agreed with medical institutions, etc. based on the Service Specification Adaptation Disclosure Form.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.

MIC "Security Management Guidelines for Cloud Service Providers Handling Medical Information version1"			Google Response (EN)
Item No		Guideline	
3.2.2	(A)4	① To prevent unauthorized access to buildings and rooms in which devices used for services are stored, security cameras and automatic intrusion monitoring devices should be installed. ② Monitoring images of security cameras and the like shall be recorded, grip shall be performed with a fixed period limit, and measures shall be taken to allow for post-referencing as needed. ③ Install surveillance cameras or the like in places where equipments, media, and the like used for services are physically stored, store the records, and check the status to confirm that there are no unauthorized entrances and exits.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0
3.2.2	(B)1	① In order to prevent peeping while the personal data is displayed, measures should be taken, such as pasting sheets of countermeasures against peeping on the operation terminal. ② Take measures so that the screen in operation does not fall within the field of view of anyone other than the operator.	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A.11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers
3.2.2	(C)1	① The equipment and media in which personal data is physically stored must be the minimum required for the provision and operation of services, and the location and inventory of the equipment and media must be periodically checked. ② Attach anti-theft chains to significant equipments, such as PCs, where the personal data resides. ③ Provide that the personal data to be consigned is not stored in the terminal used for operation and maintenance in the operation grip regulations of the company, etc.	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A.11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers
3.2.3	(A)1	① Issue accounts so that users of information systems can be identified and identified. (The ID is not shared by a plurality of users, except for the ID (non interactive ID) used by the information systems to use other information systems.) ② Authentication is performed to prevent user spoofing and the like. ③ Users include not only those who use services at medical institutions, but also those who operate or develop information systems, or those who have grip authority. ④ Issue of IDs to persons who are engaged in the operation or development of information systems or who have grip authorities is required to be minimized, and the information systems should be periodically inventoried.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001: 2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
3.2.3	(A)2	① When a combination of a user ID and a password is used to identify and authentication an individual, measures are taken to keep the user ID and the password known only to the individual. Specifically, the following measures are taken. ・When an initial password is issued to a user, access to the information system is prohibited unless the password is changed at the time of initial use. ・Passwords other than the initial password are set by the user himself or principal, and the user is requested to set the contents which can be known only by the user himself or herself. ・When a password is set, a plurality of character types (alphanumeric characters, uppercase letters, lowercase letters, symbols, etc.) are used, and a rule is made up of character strings or the like having a sufficiently secure length, such as eight characters or more. ② Actions are taken to realize the following rules related to password authentication. ・A certain refractory time is set for re-entry when password entry is unsuccessful. ・When the number of failed password re-entries exceeds a certain number, re-entry is not accepted for a certain period of time. ③ A valid period that satisfies sufficient security is set for the password. However, when the user is a patient or the like, not only is the user particularly prompted not to use the password used in another service, but the service provider does not request the patient or the like to change the password periodically. ④ Even in the case where the authentication is not based on the ID and the password, the security equivalent to or more than that described above is ensured.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001: 2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
3.2.3	(A)3	① The password information of the user is grip by an encryption method such as storing the password information with hash values. ② When introducing products to be used for services, not only are initial passwords changed, but necessary accounts are inventoried, and unnecessary initial passwords are deleted. ③ When the user forgets the ID and password, the user is notified or reissued according to a procedure (including identification) prepared in advance. ④ When information such as passwords is leaked, or when the information is leaked due to hit from an unauthorized third party, the ID is immediately invalidated, and new log-in information is reissued based on the procedures prepared in advance, and the user is promptly notified. ⑤ When there is a risk of leakage of information such as a password, a measure is taken so that the password can be invalidated and changed after notifying the user himself of the fact. ⑥ For passwords set by users, quality standards including content that is hard to be easily estimated by third parties shall be formulated, and operations shall be carried out based on these standards. ⑦ Perform grip of user passwords to ensure security when changing passwords so that previously set passwords cannot be set. ⑧ Agree with medical institutions etc. based on the Service Specification Adaptation Disclosure Form for the password policy established in the company.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001: 2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.

MIC "Security Management Guidelines for Cloud Service Providers Handling Medical Information version1"			Google Response (EN)
Item No		Guideline	
3.2.3	(A)4	① Authentication related to the use of an information system by a person engaged in the operation or development of the information system or a person having the grip person authority is performed by a method having an authentication strength of two or more factor authentication. ② Agree with medical institutions etc. on the authentication method to be adopted for user authentication based on the service specification compliance disclosure document. ③ When an authentication method using a fixed ID and password is adopted for user authentication, an effort is made to provide a function that can cope with adoption of an authentication method that does not rely solely on a fixed ID and password. The MHLW Guidelines describe that two-factor authentication is assumed to be "C. Minimum Guidelines" in Chapter 6.5 of the MHLW Guidelines after about 10 years from the release of the 5th Edition of the MHLW Guidelines (May 2017). ④ Alternative means and procedures for temporarily authenticating when some physical medium, physical information or the like is required for user authentication even if there is no exceptionally such medium or the like shall be defined in advance. ⑤ In the case where the alternative means and procedure are used, the difference in risk from the case of the original user authentication method is minimized. ⑥ Records are made to enable later tracing even when information systems are used by alternative methods and procedures, and this is grip. ⑦ In addition, the temporary user authentication method is agreed with medical institutions based on the Service Specification Adaptation Disclosure Form.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001: 2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
3.2.3	(B)1	① Measures should be taken to classify medical information and other information. ② For medical information, access control should be performed according to the information category. ③ When providing services with resources using virtualization technologies, measures are taken to ensure that section grip can be performed logically. ④ Based on the Service Specification Adaptation Disclosure Form, agree with medical institutions to set up categories of information assets by medical institutions and to respond to access control settings.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001: 2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
3.2.3	(B)2	① The service includes functions that enable access control, such as access authority and extent, for each medical worker and related job category. ② Settings of access control according to the job category of the user of the medical institution, etc. shall be indicated to the medical institution, etc., and necessary consultations shall be made with the medical institution, etc. and agreements shall be agreed, including sharing of roles related to the work to be actually set up. The provider agrees with medical institutions to provide information related to access control based on the Service Specification Adaptation Disclosure Form. ③ Operate the access grip in accordance with the operation grip regulations, and provide documentations in response to requests from medical institutions. Conditions related to the provision of data should be agreed with medical institutions based on the Service Specification Compliance Disclosure Form.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001: 2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
3.2.3	(B)3	① Services include the ability to grip medical-of-care informations on a patient-by-patient basis.	N/A
3.2.3	(C) (a)1	① When a general-purpose input terminal such as a PC is used to prepare a document or the like containing medical information subject to the e-document law, the following matters are agreed with medical institutions or the like on the basis of the service specification conformance disclosure document. ・Specifications related to identification and authentication of the inputer and determinant, including the availability of access control according to functional authority of medical institutions, etc.	N/A
3.2.3	(C) (a)2	① When a specific device or system, such as a medical examination system or a medical image filing system, is used to prepare a document or the like containing medical information subject to the e-document law, the following matters are agreed with medical institutions based on the service specification compliance disclosure document. ・Sharing of roles relating to the construction of interfaces in cooperation with services	N/A
3.2.3	(C) (b)2	① When a general-purpose input terminal such as a PC is used to prepare a document or the like containing medical information subject to the e-document law, the following matters are agreed with medical institutions or the like on the basis of the service specification conformance disclosure document. ・Specifications related to the defined registration information (identification information such as the names of the input person and the confirmation person, and the date and time of creation using a reliable time source) ・Specifications on whether or not to confirm the input contents before confirming the record ・Specifications for authority to confirm records ・Specifications related to functions for adding and deleting fixed records ・Specifications related to the function of restoring the original state of the established record ・Specifications for Auto Defined Recording Functions, etc. ・Specifications for functions of alternative confirmation authority	N/A
3.2.3	(C) (c)1	① The service for handling medical information requiring authenticity includes a function of collating the contents before and after the update, such as saving the data before and after the update, or saving the update history, when updating the medical record or the like which has been decided once.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001: 2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google has implemented monitoring tools to detect and report application vulnerabilities. Google also maintains user access logs for privileged access and for access to user data. Logical access to audit logs is restricted to authorized personnel.
3.2.3	(C) (c)2	① A service for handling medical information requiring authenticity includes a function of storing an update history when updating a medical record or the like which has been determined once, and identifying the order of updating.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001: 2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google has implemented monitoring tools to detect and report application vulnerabilities. Google also maintains user access logs for privileged access and for access to user data. Logical access to audit logs is restricted to authorized personnel.

MIC "Security Management Guidelines for Cloud Service Providers Handling Medical Information version1"			Google Response (EN)
Item No		Guideline	
3.2.3	(C) (d)	① On the basis of the service specification conformance disclosure document, agree with medical institutions on the functions and operation methods related to accounts and authority setting for performing proxy entry in a service that handles medical information requiring authenticity. ② The service for handling medical information requiring authenticity includes a function of recording the contents of proxy entry (proxy and recipient, record of proxy target, date and time of proxy). ③ The service for handling medical information requiring authenticity includes a function related to the confirmation operation (approval) after the proxy entry.	N/A
3.2.3	(D)1	① Record access to the information system and preserve it for a certain period of time. ② The access record includes an ID of access, an access time, an access time, an access target (information subject unit), and the like. ③ If you do not have the access record function, agree with medical institutions based on the service specification conformance disclosure document. ④ If the medical information to be handled has a statutory retention period, access records or alternative records for medical records should have a retention period greater than the legal period. ⑤ Agree with medical institutions based on the Service Specification Adaptation Disclosure Form on the retention period of medical information for which the statutory retention period specified in ii has elapsed and medical information for which the legal retention period has not been set. The grip method of access records in this section shall be handled in accordance with medical information that has a statutory retention period in principle when a retention period is set in the Service Specification Conformance Disclosure Form. ⑥ Regarding records of access by persons engaged in the operation or development of information systems or persons having grip authority, periodic reviews are made to ensure that there is no unauthorized access, etc. ⑦ Agree with medical institutions on the provision of information on (ii) on the basis of the service specification conformance disclosure document.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001: 2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google has implemented monitoring tools to detect and report application vulnerabilities. Google also maintains user access logs for privileged access and for access to user data. Logical access to audit logs is restricted to authorized personnel.
3.2.3	(D)2	① Restrict access to the resource in which the access record is stored to prevent unauthorized access. ② Ensure adequate space for storage of access records and ensure availability and integrity access records. ③ Actions are taken to prevent tampering, such as encrypting access records or periodically recording them on non-recordable media.	Google is certified to the ISO27001 Standard, which regulates "Cryptography" (ISO 27001:2013, Annex A.10) Customer data that is uploaded or created is encrypted at rest. We use several layers of encryption to protect customer data; adding redundant data protection and allowing us to select the optimal approach based on application requirements. Google publishes details about encryption and key management options for its Google Cloud Platform and G Suite products. To read more about key management and encryption, please see: https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including development of appropriate encryption measures.
3.2.3	(D)3	① In order to ensure the reliability of the time of the access record, synchronization between the time of the information system and the standard time or equivalent time information provided by the trusted authority is performed daily or more frequently.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001: 2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google has implemented monitoring tools to detect and report application vulnerabilities. Google also maintains user access logs for privileged access and for access to user data. Logical access to audit logs is restricted to authorized personnel.
3.2.3	(E)1	① The Operation grip Regulations and other regulations specify that measures are to be taken to prevent clearing screens, etc. on the operation and maintenance terminals, etc. of services. ② A surveillance camera or the like is used to appropriately monitor the area where the service operation and maintenance terminal or the like is installed. ③ Based on the service specification conformance disclosure document, agree with medical institutions on measures to prevent information leakage such as clear screens to user terminals that can refer to medical information installed in medical institutions. ④ In order to reduce the risk of hijacking a terminal or a session, a session for which a certain interruption time has elapsed after the user logs on can be blocked or forcibly logged off. ⑤ Concrete applications of the actions ④ to user terminals at medical institutions are agreed with medical institutions based on the Service Specification Adaptation Disclosure Form.	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A.11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers
3.2.3	(F)1	① When constructing an information system, establish procedures to prevent viruses, malware, etc. from being mixed, and construct the system in accordance with the procedures. ② The pattern definition file of the anti-virus software is always updated to the latest one. ③ When building an information system, if it is necessary to bring in or download a program from an external medium, implementation the latest anti-virus software in advance. In addition, the latest security patch is applied in consideration of the degree of influence on the information system. ④ In cases where service usage environments are subject to hit by viruses, etc., the impact of service provision is promptly made known to healthcare institutions, etc., and the required measures, etc. are sought. ⑤ Information on information systems vulnerabilities is acquired from information sources such as the JPCERT Coordination Center (JPCERT/CC), the Cabinet Cyber Security Center (NISC), and the Institute for Information Processing of Independent Administrative Organizations (IPA) periodically and when needed, and confirmed.	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001:2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/.
3.2.3	(F)2	① When an external network is connected to a device that stores medical information, a security gateway (a firewall, a router, or the like installed at the boundary of the network) is installed, and access control of each network interface is performed based on established policies such as limitation of a connection destination, limitation of a connection time, and the like. ② An intrusion detection system (IDS), an intrusion prevention system (IPS) and the like are introduced at the boundary of a network connected to medical institutions and the like to detect an unauthorized event on the network, or to block unauthorized traffic. ③ The intrusion detection system or the like updates the signature and detection rules and applies security patches to the software so that the intrusion detection system or the like can cope with the latest hit and unauthorized accesses at all times. ④ When a device cannot be installed at a network boundary, such as when hosting is used, the same control is performed in each information processing apparatus.	Google has implemented network and host base tools to detect and respond to potential security incidents. Google maintains automated log collection and analysis tools to support investigations.
3.2.3	(G)	① Based on the Service Specification Adaptation Disclosure Form, agree on the response time (general display speed, display time of search results, etc.) when medical institutions use the service.	N/A
3.2.3	(H)1	① Actions should be taken to provide the remaining amount of storable resources that can be used by each medical institution at any time. ② When medical institutions use the service, agree with medical institutions on information on available resources (storage capacity, usable period, risk, backup frequency, backup method, etc.) on the basis of the service specification conformance disclosure document. ③ Include the location (inside, portable medium) where the information system stores the information, storage capacity for each location, storage time, risks, etc. in the operation grip regulations, etc. ④ In the case of using the cloud service provided by another provider, similar information is collected and handled. When using a cloud service industry on a virtualization technology, the cloud service provider checks information about resources that can be used under contract with other operators. ⑤ Education employees about the grip methods specified in the Operation grip Rules in step ii. ⑥ For the service-related consignee as well, the service provider shall be requested to respond to the grip methods specified in the Operation grip Rules (3).	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing a process to support data file management activities.

MIC "Security Management Guidelines for Cloud Service Providers Handling Medical Information version1"			Google Response (EN)
Item No		Guideline	
3.2.3	(H)2	① Obtain a backup of the information system based on the results of the risk analysis performed in 3.2.1(2)(c)4.①. Determine what backups should be obtained, how often they should be obtained, how often they should be stored, how they should be stored, how they should be grip, etc. and include the details in the Operation grip Rules, etc. ② Regarding the backups obtained according to (1), perform periodic checks required for the grip methods of the recording medium to confirm that the recorded content is not tampered with or destroyed. ③ For the backup to be stored in the recording medium, the backup content, the use starting date, and the use ending date are clarified based on the characteristics of the medium (tape/disk, capacity, etc.), and the grip is made. ④ When the end date of use of the backup recording medium as the target is approaching, the contents thereof are copied to another medium or the like before the end date. ⑤ Include the procedures in (1) to (4) in the operation grip regulations, etc. and provide the required training to employees, etc. and subcontractors. ⑥ Agree with medical institutions to provide backup-related information based on the Service Specification Compliance Disclosure Form.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing a process to support data file management activities.
3.2.3	(H)3	① With regard to information systems, networks, and the like, redundancy measures necessary for continuing services should be taken so as not to affect normal medical care and the like. ② When information such as medical records is stored in a recording equipment such as a hard disk, countermeasures against disk failures equivalent to RAID-1 or RAID-6 or more should be taken. ③ Based on the service specification conformance disclosure document, agree on the level of assurance of service continuity in the event of failure, etc. with medical institutions. ④ Based on the service specification conformance disclosure document, agree with medical institutions on alternative measures on the side of medical institutions, etc. to enable continuation of medical care, etc. even in the event of disability.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
3.2.3	(H)4	① In cases where information is damaged, actions are taken to recover quickly, and the details and procedures should be included in the Operation grip Rules, etc. ② Include in the Operation grip Regulations, etc. the countermeasures to be taken when it is difficult to recover the damaged data by the measures shown in (1). ③ The scope of responsibility and exemption conditions for the damaged information are agreed with medical institutions based on the Service Specification Adaptation Disclosure Form.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing a process to support data file management activities.
3.2.3	(H)5	① Periodically confirm that the readability of equipments, media, etc. that store medical information is ensured. ② In cases where it may become difficult to ensure the readability of equipments and media that store medical information to be commissioned (deterioration of media, support of readers, etc.), take alternative measures promptly to ensure readability.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
3.2.3	(I)1	① A configuration diagram of equipment and software in an information system is created. ② Create a network configuration diagram of the information system. ③ Prepare documents with descriptions of system requirements for the devices included in the configuration diagrams created in (1) and (2). ④ Documentations relating to the specifications of updates and the like of the equipment, software, and the like constituting the information system and the update history thereof are prepared. ⑤ In order to submit the data prepared in steps (1) to (4) in response to a request from a medical institution, etc., agree with the medical institution on the content, scope, conditions, etc. of the disclosure based on the service specification compliance disclosure document.	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001:2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.

MIC "Security Management Guidelines for Cloud Service Providers Handling Medical Information version1"			Google Response (EN)
Item No		Guideline	
3.2.3	(I)2	① Include the measures and procedures related to the quality grip of the equipment and software used for services in the operation grip regulations, etc. ② Educations employees about the quality grip of equipment and software used for services. ③ Request the service-related consignee to respond to the quality-of-service grip required by its own company to meet the requirements of the main guideline. ④ Include the content, procedures, etc. of internal audits related to system configuration and software operation status in the operation grip regulations, etc.	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001:2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
3.2.3	(J)1	① For security measures necessary when medical institutions use wireless LANs when using services that handle medical information, agree with medical institutions on roles sharing among cloud service operators based on the Service Specification Adaptation Disclosure Form.	N/A
3.2.3	(J)2	① When providing services including the use of IoT equipments, agree with medical institutions on the responsibility division with medical institutions based on the service specification conformance disclosure document. ② When a service including the use of an IoT equipment is provided, the state of access to the medical information system by the IoT device is recorded, and the absence of unauthorized access is periodically monitored. ③ When services including the use of IoT equipments are provided, information on vulnerabilities to the IoT devices expected to be used is periodically collected and necessary measures are taken.	N/A
3.2.4	(A)1	① For personnel (employees, dispatchers, etc.) engaged in the provision of services, the content of confidentiality obligations should be included in employment contracts or dispatch contracts, or should be included in work rules, etc.	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.2.4	(A)2	① Education and train personnel involved in providing services on personal data policy and personal data safety grip. ② This education and training is performed at the beginning of work and periodically after work.	Google is certified to the ISO27001 Standard, which regulates "Information Security Awareness, Education and Training" (ISO 27001:2013, Annex A.7.2.2), Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All Google contractors undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new contractors agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.
3.2.4	(A)3	① Confidentiality obligations related to personal data handled during work should be included in employment contracts or dispatch contracts or included in work rules, etc. when personnel engaged in the provision of services leave the office. ② For the personal data where the personnel involved in the provision of the services had grip in the work, request return at the time of departure (including internal change), and confirm that the systems grip personnel were returned. ③ The confidentiality obligations of personnel involved in the provision of the service at the time of retirement or after the end of contract shall be included in the education and training in section 2 above.	Google is certified to the ISO27001 Standard, which regulates ""Terms and Conditions of Employment"" (ISO 27001:2013, Annex A.7.1.2), Hiring practices controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google performs background checks on new hires as permitted by local laws
3.2.4	(A)4	① Include appropriate penalties in employment contracts or dispatch contracts or in work rules, etc. for employees, dispatch operators, etc. who violate the above-mentioned 1-3.	Google is certified to the ISO27001 Standard, which regulates ""Terms and Conditions of Employment"" (ISO 27001:2013, Annex A.7.1.2), Hiring practices controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google performs background checks on new hires as permitted by local laws
3.2.4	(A)5	① On the basis of the Service Specification Adaptation Disclosure Document, agree with medical institutions to provide data on the status of education and training for personnel engaged in the provision of services, the status of responses to confidentiality obligations, etc.	Google is certified to the ISO27001 Standard, which regulates ""Terms and Conditions of Employment"" (ISO 27001:2013, Annex A.7.1.2), Hiring practices controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google performs background checks on new hires as permitted by local laws
3.2.4	(B)1	① When re-entrusting information systems, explain the re-entrusting information systems to grip providers such as healthcare institutions in advance, and clarify the system in the contract related to the re-entrustment. ② The subcontractor is required to comply with the same personal data guidelines as its own. ③ Include confidentiality obligations related to the consignment business in the contract related to the re-consignment. ④ Confirm with the subcontractor that the subcontractor personnel has the same confidentiality obligation as that of the company. ⑤ Confirm that the subcontractor has taken the safety grip measures specified in this guideline.	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.2.5	(A)1	① Procedures for discarding equipments, media, etc. that store information used for services include measures to prevent restoration of original data due to irreversible destruction, deletion, etc. ② When information is discarded, in response to a request from a medical institution, report the implementation details including the person in charge of implementation and the method of deleting the information (such as demagnetization and physical destruction of an electro-magnetic recording medium) to the medical institution, and submit the discard record. ③ Based on the Service Specification Adaptation Disclosure Form, agree on the measures to be taken in (1) and the conditions necessary to provide the data in (2).	Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" (ISO 27001:2013,Annex A.11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.
3.2.5	(A)2	① When re-entrusting information systems, explain the re-entrusting information systems to grip providers such as healthcare institutions in advance, and clarify the system in the contract related to the re-entrustment. ② The subcontractor is required to comply with the same personal data guidelines as its own. ③ Include confidentiality obligations related to the consignment business in the contract related to the re-consignment. ④ Confirm with the subcontractor that the subcontractor personnel has the same confidentiality obligation as that of the company. ⑤ Confirm that the subcontractor has taken the safety grip measures specified in this guideline.	Google is certified to the ISO27001 Standard, which regulates "Supplier Relationships" (ISO 27001:2013, Annex A.15). Information security oversight and management controls, including vendor security practices are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google directly conducts virtually all data processing activities to provide our services. However, Google may engage some third-party suppliers to provide services related to Cloud Platform, including customer and technical support. Prior to onboarding third-party suppliers, Google conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms.

MIC "Security Management Guidelines for Cloud Service Providers Handling Medical Information version1"			Google Response (EN)
Item No		Guideline	
3.2.6	(A)1	① When a person who is engaged in maintenance of an information system and a person who has grip authority accesses the information system for the purposes of the task, the access is performed by a accounts issued for each factor. ② The tasks performed by the accounts specified in (1) should be logged and saved in such a way that the accessed personal data can be identified.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001: 2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google has implemented monitoring tools to detect and report application vulnerabilities. Google also maintains user access logs for privileged access and for access to user data. Logical access to audit logs is restricted to authorized personnel.
3.2.6	(A)2	① Persons engaged in the maintenance of information systems and those with grip authorities shall strictly grip information systems so as not to leak accounts for business use.	N/A
3.2.6	(B)1	① Prepare procedures for maintenance operations by remote maintenance, and take safety grip actions to prevent unauthorized access to data systems. ② Records of maintenance work by remote maintenance are obtained by access logs, etc., and the systems grip person confirms the content promptly. ③ When the maintenance of the information system necessary for the service provision is performed by remote maintenance, agree with the medical institution etc. on the basis of the service specification conformance disclosure document.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001: 2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google has implemented monitoring tools to detect and report application vulnerabilities. Google also maintains user access logs for privileged access and for access to user data. Logical access to audit logs is restricted to authorized personnel.
3.2.6	(B)2	① Records and grip the results of operations performed in the maintenance of information systems using operation logs and the like. ② The status of the accessed medical information is reviewed using the obtained operation log or the like.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001: 2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google has implemented monitoring tools to detect and report application vulnerabilities. Google also maintains user access logs for privileged access and for access to user data. Logical access to audit logs is restricted to authorized personnel.
3.2.6	(B)3	① Agree with medical facilities on the basis of the service specification conformance disclosure document for the response when the maintenance work of the information system is carried out in the institutions such as medical institutions.	N/A
3.2.6	(B)4	① When the maintenance work of the information system is performed, in principle, the information system should be notified to grip persons such as medical institutions in advance of the work and after the work by a document or the like. Based on the Service Specification Compliance Disclosure Form, agree with medical institutions on tasks that require prior understanding and how to deal with cases where prior understanding of the tasks cannot be obtained. ② The advance notice in (1) specifies the extent affected by the maintenance work, and includes the prediction of the time required for the original state restoration assuming the case where the maintenance work is not completed. ③ When carrying out the maintenance work, take appropriate measures to prevent medical institutions from becoming unavailable, and include the procedures in the operation grip regulations. ④ Procedures specified in (3) are indicated to medical institutions, etc. and agree with medical institutions, etc. on the basis of the service specification conformance disclosure document. Agree with medical institutions based on the Service Specification Adaptation Disclosure Form about items required for maintenance based on this procedure. ⑤ When medical institutions need to respond to the procedure indicated in ii), agree with the medical institutions based on the service specification conformance disclosure document. ⑥ After the maintenance operation is performed, reports are made to medical institutions, etc. and the grip personnel of medical institutions, etc. are checked. The response to this procedure is agreed with medical institutions, etc. on the basis of the service specification conformance disclosure document.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001: 2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google has implemented monitoring tools to detect and report application vulnerabilities. Google also maintains user access logs for privileged access and for access to user data. Logical access to audit logs is restricted to authorized personnel.
3.2.6	(C)1	① When checking the operation of information systems, data for testing should be used instead of data including personal data accepted in principle. ② Procedures including confirmation of operations by personnel and consignees for whom confidentiality obligations as shown in 3.2.4 are imposed should be defined when data including consigned personal data is inevitably used for confirmation of operations of information systems. ③ In order to confirm the operation of the information system, when the commissioned personal data must be used, agree with the medical institution based on the service specification conformance disclosure document.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001: 2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google has implemented monitoring tools to detect and report application vulnerabilities. Google also maintains user access logs for privileged access and for access to user data. Logical access to audit logs is restricted to authorized personnel.
3.2.6	(C)2	① When it is necessary to bring a device or the like storing medical information outside the organization of a medical institution or a cloud service provider (including a subcontractor) for the purpose of maintenance (for example, repair of the device), the procedure should be formulated. ② Based on the service specification conformance disclosure document, agree with medical institutions on the procedures and information provision conditions specified in (1).	Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" ((ISO 27001: 2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" ((ISO 27001:2013,Annex A. 11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.
3.2.6	(D)1	① For data items such as medical records, the standards for the field of health and medical information in the MHLW (hereinafter referred to as "MHLW standards") shall be adopted. ② Data items for which the MIC standards have not been established shall be in an easy-to-convert data format and agree with medical institutions based on the Service Specification Compliance Disclosure Form.	N/A
3.2.6	(D)2	① The information systems are provided with functions and validation methods that prevent changes in information in medical records, such as record grip methods and actions to be taken when changing the master table of medical information. ② Agree with medical institutions, etc. on the procedures for updating and migrating information systems when it is difficult to provide the functions shown in (1) based on the service specification conformance disclosure document.	Google is certified to the ISO27001 Standards, which regulates "Operational Procedures and Responsibilities" (ISO 27001:2013, Annex A.12.1) and "Network Security" (ISO 27001:2013, Annex A.13.1). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. System changes that may affect security, availability, processing integrity, or confidentiality are communicated to management and users who will be affected.
3.2.6	(D)3	① When upgrading or changing the data format or the transfer protocol, confirm the impact on the use of the service. ② If it is found that there is an impact on the use of the service as a result of (1), the health care institution shall provide notice of version upgrade or change assuming a period sufficient for the health care institution, etc., and shall provide concrete information on the measures necessary for the response. ③ This section is based on data linkage with other information systems. Agree with medical institutions to provide information to ensure compatibility with medical institutions based on the Service Specification Adaptation Disclosure Form. ④ When the medical institution or the like terminates the use of the service as a result of the change of the data format and transfer protocol, the measures shown in 3.4 shall be taken.	Google is certified to the ISO27001 Standards, which regulates "Operational Procedures and Responsibilities" (ISO 27001:2013, Annex A.12.1) and "Network Security" (ISO 27001:2013, Annex A.13.1). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. System changes that may affect security, availability, processing integrity, or confidentiality are communicated to management and users who will be affected.
3.2.6	(D)4	① Regarding the equipment related to the information system used for the service, the inspection concerning the deterioration state is periodically carried out, and necessary measures are taken. ② For information systems used for services, when support by providers of equipment, software, etc. is terminated, analyze the extent of impact on the services and take necessary measures. ③ In cases where it becomes difficult to provide some or all of the services due to deterioration of equipment or termination of support of equipment or software at providers, etc., or where there is a change in the services, the information system used for the services shall be notified with a sufficient period for the medical institutions, etc. to respond in addition to taking measures to minimize the impact on the medical institutions, etc. ④ Under the Service Specification Compliance Disclosure Form, agree with medical institutions on the details and conditions of the response to medical institutions when some or all of the services are stopped or changed.	Google is certified to the ISO27001 Standards, which regulates "Operational Procedures and Responsibilities" (ISO 27001:2013, Annex A.12.1) and "Network Security" (ISO 27001:2013, Annex A.13.1). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. System changes that may affect security, availability, processing integrity, or confidentiality are communicated to management and users who will be affected.

MIC "Security Management Guidelines for Cloud Service Providers Handling Medical Information version1"			Google Response (EN)
Item No		Guideline	
3.2.6	(D)5	① Equipments and software related to information systems used for services handling medical information shall be decided in view of ensuring future compatibility, and risks in case of changes in standard specifications etc. after the service is provided shall also be examined. ② When a service is provided using a cloud service provided by another cloud service provider, measures are taken to prevent a problem from occurring in the provider's service provision even when another cloud service provider stops the service. If some or all of the services provided by another cloud service provider are stopped or changed (minor version upgrades are not included) due to the stoppage or change of the cloud service of another cloud service provider, "4. Measures are taken to cope with the problems described in sections (2) to (4) of "Measures against degradation of devices used in services". ③ When updating the equipment or software related to the information system used for the service handling medical information, or when changing the cloud service of another cloud service provider to be used, consider (1) and (2).	Google is certified to the ISO27001 Standard, which regulates "Supplier Relationships" (ISO 27001:2013, Annex A.15). Information security oversight and management controls, including vendor security practices are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google directly conducts virtually all data processing activities to provide our services. However, Google may engage some third-party suppliers to provide services related to Cloud Platform, including customer and technical support. Prior to onboarding third-party suppliers, Google conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms.
3.2.6	(E)1	① When a system change such as maintenance of an information system occurs, agree with medical institutions on the extent and content of reports to medical institutions, etc. and conditions related to the provision of the information, based on the service specification compliance disclosure document.	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.2.6	(E)2	① When part or all of the maintenance of information systems is entrusted to external operators, the external operators are requested to respond to the operational grip regulations and safety grip actions that are being implemented by the external operators. ② Regarding the implementation status of (1), request and confirm the report from external operators on a contract-by-contract basis or on a regular basis.	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.2.7	(A)1	① Policies and rules related to the removal (including removal from the consignor) of equipments and media that store information related to services (consignment information, information related to information systems, etc.) shall be defined in the Operation grip Rules. ② The term "take-out" in (i) includes not only physical taking-out but also send to the outside through a network. ③ Agree with medical institutions, etc. based on the service specification conformance disclosure document for the contents defined in (1).	Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" ((ISO 27001:2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" ((ISO 27001:2013,Annex A.11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.
3.2.7	(A)2	① For recording media and recording equipment used for services, include the following in the Operation grip Rules.・Grip System and grip Methods・Treatment of Recording Media and Recording Devices・Policies and rules related to the removal (including removal from the consignor) of equipments and media that store information related to services (consignment information, information related to information systems, etc.) (In addition to physical removal, "removal" includes transmission to the outside via a network).・When information on services is taken out, the equipment and media that store the information are stolen or lost (in addition to physical theft or loss of equipment and media at the time of take-out, system grip is sent to the outside that is not approved by the system operator (including malicious responses by third parties, erroneous transmissions by employees, etc.))・Connection conditions for connecting to external networks, safety grip actions, etc. (Specific measures to prevent leakage or tampering of stored data (anti-malware measures, encryption, implementation of firewalls, etc.)	Google is certified to the ISO27001 Standard, which regulates "Documented Operating Procedures" (ISO27001:2013, Annex A.12.1.1). Google maintains robust internal documentation and maintains an ISMS, per ISO27001 requirements. All documentation in on systems that are replicated and subject to backup. Customers using Google Cloud Platform, retain all rights and responsibilities to configure and manage their environment, including development of operational guidance.
3.2.7	(A)3	① Education employees about the contents described in "2. Response to Recording Media and Recording Equipments for Services". ② Compliance with the above operation grip regulations is also required for the subcontractor.	Google is certified to the ISO27001 Standard, which regulates "Information Security Awareness, Education and Training" (ISO 27001:2013, Annex A.7.2.2), Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All Google contractors undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new contractors agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.
3.2.7	(A)4	① Based on the Service Specifications Adaptation Document, we agree with health care institutions to address the operational grip regulations for taking out the data shown in Section 2, "Response to Recording Media and Recording Equipments for Services" and Section 3, "Response to Employees and Submitters".	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.2.7	(B)	① For devices and media that store information on services, perform register grip, etc. and periodically check the location of the devices and media.	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001:2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
3.2.7	(C)1	① Set a startup password for a device or the like used for a service. ② Measures should be taken to prevent an unauthorized activation of a device by a third party, such as setting an activation password that is hard to guess and periodically changing the activation password according to the characteristics of the device. ③ A plurality of authentication elements are combined for login and access to an information device that stores information related to a service.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.

MIC "Security Management Guidelines for Cloud Service Providers Handling Medical Information version1"			Google Response (EN)
Item No		Guideline	
3.2.7	(C)2	① Procedures for taking out equipments, media, etc. that store information related to services include such things as applying encryption measures to the devices, media itself, applying encryption measures to the stored information, and setting passwords.	Google is certified to the ISO27001 Standard, which regulates "Cryptography" (ISO 27001:2013, Annex A.10) Customer data that is uploaded or created is encrypted at rest. We use several layers of encryption to protect customer data; adding redundant data protection and allowing us to select the optimal approach based on application requirements. Google publishes details about encryption and key management options for its Google Cloud Platform and G Suite products. To read more about key management and encryption, please see: https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including development of appropriate encryption measures.
3.2.7	(C)3	① When a device storing information on a service is taken out, a minimum number of applications necessary for the purpose of taking out the device are installed. ② Determine the procedure for installing an application when a device that stores information related to a service is taken out.	N/A
3.2.7	(C)4	① Use of individual ownership equipment such as employees for the purpose of providing services (including development, maintenance, and operation) shall be prohibited. ② Personal countermeasures related to the use of services by devices owned by users, agree with medical institutions, etc. on the basis of the service specification conformance disclosure document. More specifically, the following contents will be referred to.・In order to prevent leakage of information from equipments owned by users, for example, it is conceivable to divide business use areas and personal use areas at the OS-level using virtual desktops so that medical institutions and others can grip the business use areas. In addition, mobile device management (MDM) and mobile application management (MAM) can be applied to strictly implement security measures equivalent to security measures for terminals owned by medical institutions and others, which are grip owned by medical institutions and others.	The Google Device Policy restricts the user and device behavior on mobile devices including application installation. For advanced use, a work profile is required which includes a restricted apps store.
3.2.7	(C)5	① In business, when a mobile terminal storing information on a service is taken out, connection to a public wireless LAN is not performed.	N/A
3.2.8	(A)1	① After clarifying the responsibility division in case of failure, agree with medical institutions on the extent of service guaranteed to operate based on the service specification conformance disclosure document.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2), and "Backup" (ISO27001:2013 Annex A 12.3.), and "Documented Operating Procedures" (ISO27001:2013, Annex A 12.1.1). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
3.2.8	(A)2	① When medical information is stored in medical institutions, agree with medical institutions to provide information on measures that can be taken by medical institutions to ensure readability in the event of a disability, based on the Service Specification Adaptation Disclosure Form.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2), and "Backup" (ISO27001:2013 Annex A 12.3.), and "Documented Operating Procedures" (ISO27001:2013, Annex A 12.1.1). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
3.2.8	(A)3	① When medical information is stored in medical institutions, agree with medical institutions on the availability and content of functions related to the output of external files required to ensure readability in the event of a disability, based on the Service Specification Adaptation Disclosure Form.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2), and "Backup" (ISO27001:2013 Annex A 12.3.), and "Documented Operating Procedures" (ISO27001:2013, Annex A 12.1.1). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.

MIC "Security Management Guidelines for Cloud Service Providers Handling Medical Information version1"			Google Response (EN)
Item No		Guideline	
3.2.8	(A)4	① In the case where medical information is stored in medical institutions, agree with medical institutions based on the Service Specification Adaptation Disclosure Form on the functions for using backup data stored in remote locations to ensure readability in the event of a disability, the provision of information required for use, conditions, and the like.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions.
3.2.8	(A)5	① Based on the Service Specification Adaptation Disclosure Form, agree on the inclusion of functions (e.g., screen printing functions, file downloading functions, etc.) in the service to support the assurance of readability of medical records and the like at medical institutions in case of emergency, and the provision of information such as security necessary for this.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2), and "Backup" (ISO27001:2013 Annex A 12.3.), and "Documented Operating Procedures" (ISO27001:2013, Annex A 12.1.1). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
3.2.8	(B)1	① Develop BCP and contention plans for services. ② The BCP and contention plan formulated in (1) should include the contents of emergency systems and service recovery procedures. ③ The contents of services based on the BCP and contention plan formulated in (1) are agreed with medical institutions based on the service specification conformance disclosure document.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
3.2.8	(B)2	① Agree with medical institutions, etc. on measures to enable emergency user accounts and emergency functions, based on the service-specification conformance disclosures. ② Periodic reviews will be made on the status of use of user accounts in emergency situations. ③ When the user accounts used in the emergency is used, measures should be taken to enable the systems grip operator and the operator to confirm this promptly. ④ For the user accounts and emergency functions that were effective in the event of an emergency, the function should be disabled immediately after returning to normal status.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2), and "Backup" (ISO27001:2013 Annex A 12.3.), and "Documented Operating Procedures" (ISO27001:2013, Annex A 12.1.1). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
3.2.8	(B)3	① Take actions to preserve logs and other records required for investigating the causes of problems in the provision of services due to cyber hit, etc. ② In case (1), the status of failures occurring in the service and the prospects for recovery should be promptly reported to medical institutions, etc. ③ In case (1), the scope and conditions of data to be provided for communication and reporting by medical institutions and other agencies should be agreed with medical institutions based on the Service Specification Adaptation Disclosure Form. ④ Applications, platforms, server storages, etc. used to provide services should be installed in locations covered by the domestic law enforcement so that the documentations provided by medical institutions to government agencies based on laws can be smoothly submitted to the agencies.	Google is certified to the ISO27001 Standard, which regulates "Information Security Policy" (ISO 27001:2013, Annex A.5) and Organization of Information Security (ISO27001:2013, Annex A.6). Information security oversight and management controls, including documentation of information security policies are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.

MIC "Security Management Guidelines for Cloud Service Providers Handling Medical Information version1"			Google Response (EN)
Item No		Guideline	
3.2.8	(B)4	① To ensure that the results of data processing performed in an emergency do not conflict after service restoration, measures should be taken to ensure the consistency of the data (e.g., stipulation of rules and verification methods).	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
3.2.9	(A)1	① In the network, measures necessary to protect information from eavesdropping, tampering, communication through wrong routes, destruction, and the like (maintenance of implementation standards and procedures of information exchange, encryption of communication, and the like) are performed. ② Take necessary measures (implementation of a server certificate, etc.) to prevent access destination spoofing (session hijacking, phishing, etc.). ③ In order to ensure the safety of the routes, we agree with medical institutions, etc. based on the service-specification conformance disclosures regarding support for IPSec + IKE, support for closed networks, etc. ④ Based on the Service Specification Adaptation Disclosure Document, agree on the extent of the cloud service provider's role in protecting against tampering such as the mixing of viruses and unauthorized messages in the network path. ⑤ When medical institutions expect to adopt closed networks for ensuring channel security, agree with medical institutions on information on the extent of closed services based on the service specification conformance disclosure document.	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001:2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/.
3.2.9	(A)2	① In the network from the medical institution to the cloud service provider, the route is checked in the necessary units such as the entrance and exit of the transmission and reception base of the medical institution, the equipment used, the functional units on the equipment used, and the users. ② In (1), mutual authentication is performed between a server or the like externally connected by a medical institution or the like and a server of a cloud service provider. ③ Regarding (1), if the operator re-entrusts the maintenance operation, measures are taken to prevent spoofing separately for the connection between the provider and the re-entrusted destination. ④ Based on the Service Specification Adaptation Disclosure Form, agree with the Medical Institute to confirm that the communication method authentication means adopted by the Medical Institute is appropriate based on 2 in Section 6.11 C of the Fifth Edition of the Health, Labour and Health Department Guidelines.	Google's security teams are committed to a strong perimeter and dedicated staff are responsible for the safety and security of Google's network infrastructure. Google conducts rigorous internal continuous testing of our network perimeter through various types of penetration exercises. In addition, Google coordinates external third party penetration testing using qualified and certified penetration testers.
3.2.9	(A)3	① Network devices, such as routers, select security targets or similar documents defined in the ISO15408 that conform to this guideline. ② Regarding routers in facilities such as medical institutions used in networks, the role sharing of cloud service providers in setting routes to prevent transmission and reception between VPNs connecting facilities through the routers should be agreed with medical institutions based on the service specification adaptation disclosure document.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Access to information resources, including data and the systems which store or process data, is authorized based on the principle of least privilege. Access to network devices is authenticated via user ID, password, security key, and/or certificate. External system users are identified and authenticated via the Google Accounts authentication system before access is granted.
3.2.9	(A)4	① Security measures against the information itself, such as encryption, are implemented between the transmission source and the transmission destination. ② When using the SSL/TLS to provide services, the actions described in TLS1. 2 should be taken. ③ In addition to (2), when medical institutions require measures to encrypt e-mails (e.g., S/MIME) and encrypt files, agree with medical institutions on the measures and conditions required to cope with the requests based on the service-specification conformance disclosures.	Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. Please see https://cloud.google.com/security/encryption-in-transit/ for more informaiton.
3.2.9	(A)5	① When connecting via an open network using the HTTPS, both the server and the client set up the TLS appropriately in accordance with the "high security type" with the highest security specified in the "SSL/TLS cryptography setting guideline". ② SSL-VPN is not used in principle. ③ In providing services, when connecting by software-based IPsec or TLS1. 2, appropriate measures should be taken for hit caused by looping between sessions (accessing closed sessions that are not legitimate routes). ④ When a user at a medical institution or the like connects by a software-type IPsec or TLS1. 2, it provides information on appropriate measures for hit by wrapping around between sessions (access to closed sessions that are not regular routes). Agree with medical institutions on the extent and conditions of information provision based on the Service Specification Adaptation Disclosure Form.	Google supports the use of open encryption methodologies. Google forces TLS for all authentication traffic. Customer data is encrypted when on Google's internal networks, in transport and at rest.
3.2.9	(A)6	① Based on the Service Specifications Adaptation Document, agree on the scope and roles of cloud service providers' responsibilities for line grip, quality, etc.	Google is certified to the ISO27001 Standard, which regulates "Communications Security" (ISO 27001:2013, Annex A.13), and "Securing Application Service on Public Networks" ISO 27001:2013, (Annex A.14.1.2). Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including management of external connections.
3.2.9	(A)7	① When a user of a medical institution or the like uses a service from the outside of the medical institution or the like, the user agrees with the medical institution or the like on the basis of the service specification adaptation disclosure document regarding the role sharing of the cloud service provider or the like for introducing a technology such as a virtual desktop or the like into the work environment of the PC used by the user of the medical institution or the like.	Google agrees contractually with providers on adherence to Google's security and privacy policies and has a vendor audit program to determine compliance.
3.2.9	(B)1	① When maintenance is performed by remote maintenance, appropriate safety grip actions such as setting up access points, restricting protocols, and access authority grip should be taken as needed.	Google is certified to the ISO27001 Standard, which regulates "Supplier Relationships" (ISO 27001:2013, Annex A.15). Information security oversight and management controls, including vendor security practices are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google directly conducts virtually all data processing activities to provide our services. However, Google may engage some third-party suppliers to provide services related to Cloud Platform, including customer and technical support. Prior to onboarding third-party suppliers, Google conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms.
3.2.9	(C)1	① Communication procedures from the start point to the end point between medical institutions in normal operation and emergency, as well as the network routes defined in Section 6.11 C of the MHLW Guidelines, 5th Edition 6.11, are clarified, and the scope of responsibility and roles of operators are agreed with medical institutions based on the Service Specification Adaptation Disclosure Form. ② The security level of the information to be exchanged is agreed with medical institutions based on the service specification conformance disclosure document so that the security level is not lowered at the receiving side. ③ In terms of accountability, grip responsibility, etc. of grip persons of medical institutions, etc., agree with medical institutions, etc. on the scope of responsibility, roles, etc. of the operators, based on the service specification Adaptation Disclosure Form.	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.2.9	(C)2	① When medical information to be grip by the service is to be viewed by the patient, the provider of the cloud service agrees with the medical institution on the terms and content of security measures to be taken by the provider of the cloud service on the basis of the service specification conformance disclosure document. ② When medical information is to be viewed by a patient or the like, the provider agrees with the medical institution or the like on the provision conditions and contents of information related to security measures to be taken in the viewing environment of the medical institution or the patient based on the service specification conformance disclosure document. ③ Based on the Service Specification Adaptation Disclosure Form, agree with medical institutions on the scope of responsibility and role of cloud service providers in accountability for the security of information systems in which the patient or the like views information.	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/

MIC "Security Management Guidelines for Cloud Service Providers Handling Medical Information version1"			Google Response (EN)
Item No		Guideline	
3.2.10	(A)	① When a signature or stamp is replaced with an electronic signature in a document or the like which is mandated to be signed or signed and stamped by law, it is made clear to medical institutions whether or not to cope with the digital certificate for signature issued by the Health and Medical Welfare Field PKI Certificate Authority. ② When providing a service that uses electronic signatures for signing and stamping as prescribed by law, using an electronic certificate issued by a certified authentication business operator in the electronic signing law other than the electronic certificate issued by the Health and Welfare Field PKI Certificate Authority, agree with medical institutions and others on the identity verification method and verification method in the service on the basis of the service specification conformance disclosure document, based on the electronic certificate issued by the Health and Welfare Field Certification Authority's PKI Certificate Authority. Note that since it is possible to satisfy the requirements of Section 2 1 of the "Law on Digital Signature and Authentication Business (Law No. 102, 2000)" without using an electronic certificate issued by an authorized certification business operator based on the regulations of the digital signature law, it is possible to confirm the identity with equal strictness, and further to ensure that administrative agencies that perform monitoring and the like can verify the digital signature, and in the case of using an electronic certificate issued by a business other than the authorized certification business operator, it is indicated that the above requirements can be guaranteed, and the identity confirmation method and the verification method in the service are agreed with medical institutions and the like based on the service specification conformance disclosure document. ③ In the case of providing a service in which signing and stamping prescribed by law are carried out by electronic signature using the digital certificate for signature in the public personal authentication service, a method of verifying the digital certificate related to the public personal authentication service in the service and the like are agreed with medical institutions and the like based on the service specification conformance disclosure document.	N/A
3.2.10	(B)	① A time stamp is attached to the information to which the electronic signature is applied. In this case, the contents and verification method of the time stamp are agreed with medical institutions based on the service specification conformance disclosure document. ② When dealing with time-stamped information, agree with medical institutions on methods for verifying the validity of the time-stamp within the statutory retention date and measures, based on the Service Specification Adaptation Disclosure Form. ③ When handling time-stamped information, agree with medical institutions on measures to be taken to preserve the information for a long time based on the Service Specification Compliance Disclosure Form.	N/A
3.2.10	(C)	① When dealing with time-stamped information, agree with medical institutions based on the Service Specification Adaptation Disclosure Document on the method of assigning time stamps to ensure the validity of electronic signatures before revocation of electronic certificates.	N/A
3.3.1		The Fifth Edition of the Guidelines for External Storage of Medical Information is listed in the "Standards for External Storage of Eight Records and Records" in the Fifth Edition of the Guidelines for Health, Labour, and Health Department Guidelines. Cloud service providers are required to satisfy these guidelines when handling medical information. External storage through cloud services is electronic storage. In this case, it is required to satisfy the authenticity, legibility, and storage specified in "7 Requirements for Electronic Storage" of the 5th edition of the Ministry of Health, Labour and Welfare Guidelines.	N/A
3.3.2		Documents that require external storage are those listed in Table 1 as specified in the External Storage Revision Notification, as shown in Chapter 3.2 of the Fifth Edition of the MHLW Guidelines. In addition, if the documents shown in Table 1 are not subject to Enforcement Notice 26 or External Storage Amendment Notice due to the expiration of the statutory retention period, etc., the documents should be handled in accordance with Chapters 7 to 9 (MHLW Guidelines Fifth Edition, Chapter 3.4) if they are to be stored externally (continued).	N/A
3.3.3	【To save to the etc. of medical institutions】	(1) Input Person and Confirmer Identification and Authentication	Google is certified to the ISO27001 Standard, which regulates "Cryptography" (ISO 27001:2013, Annex A.10) Encryption is used to protect user authentication and administrator sessions transmitted over the Internet. Remote access to Google corporate machines requires a Google issued digital certificate installed on the connecting device and two-factor authentication. Google publishes details about encryption and key management options for its Google Cloud Platform and G Suite products.
		(2) Establishment of record establishment procedure and record of identification information	Google is certified to the ISO27001 Standard, which regulates ""Access Control"" (ISO 27001: 2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report.
		(3) Save Update History	Google is certified to the ISO27001 Standard, which regulates ""Access Control"" (ISO 27001: 2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report.
		(4) Authorization function for proxy entry	N/A
		(5) Quality grip of equipment and software	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001:2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
	【To save data outside the etc. of healthcare institutions via networks】	(1) Performing mutual authentication to recognize that the other party of communication is legitimate	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001:2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/.
		(2) To ensure that they have not been "tampered with" on the network	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001:2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/.

MIC "Security Management Guidelines for Cloud Service Providers Handling Medical Information version1"			Google Response (EN)
Item No		Guideline	
		(3) Restricting Remote Login Functionality	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001: 2013, Annex A.9). Monitoring tools send automated alerts to operational personnel based on predetermined criteria. Incidents are escalated per policy.
3.3.4	【Contents common to save locations】	(1) Location grip	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001: 2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
		(2) Grip of reading tools	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing a process to support data file management activities.
		(3) Response time for reading purposes	Google provides customers with uptime metrics and industry standard audit reports and certifications.
		(4) Ensuring redundancy as a measure against system failures	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing a process to support data file management activities.
	【To save to the etc. of medical institutions】	(1) Backup server	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing a process to support data file management activities.

MIC "Security Management Guidelines for Cloud Service Providers Handling Medical Information version1"			Google Response (EN)
Item No	Guideline		
		(2) External output to ensure readability	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2), and "Backup" (ISO27001:2013 Annex A 12.3.), and "Documented Operating Procedures" (ISO27001:2013, Annex A 12.1.1). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
		(3) Reading function using remote data backup	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2), and "Backup" (ISO27001:2013 Annex A 12.3.), and "Documented Operating Procedures" (ISO27001:2013, Annex A 12.1.1). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
	【To save data to the outside via a network】	(1) Ensuring readability of medical records expected to be urgently needed	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2), and "Backup" (ISO27001:2013 Annex A 12.3.), and "Documented Operating Procedures" (ISO27001:2013, Annex A 12.1.1). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
		(2) Ensuring readability of medical records that are not required to be urgent	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2), and "Backup" (ISO27001:2013 Annex A 12.3.), and "Documented Operating Procedures" (ISO27001:2013, Annex A 12.1.1). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
3.3.5	【To save to the etc. of medical institutions 】	(1) Prevention of information destruction and confusion by viruses and inappropriate software	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001:2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/.

MIC "Security Management Guidelines for Cloud Service Providers Handling Medical Information version1"			Google Response (EN)
Item No	Guideline		
		(2) Prevention of loss and destruction of information due to inappropriate storage and handling	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0
		(3) Preventing unreadable or incomplete reading due to deterioration of recording media and equipment	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing a process to support data file management activities.
		(4) Prevention of unrecoverability due to inconsistencies in media, equipment, and software	Google is certified to the ISO27001 Standard, which regulates "Logging and Monitoring" (ISO 27001:2013, Annex A.12.4). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Integrity checks are in place at the application level and file system level to ensure data integrity.
		(1) Prevention of loss and destruction of information due to inappropriate storage and handling	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing a process to support data file management activities.
		(2) Preventing unreadable or incomplete reading due to deterioration of recording media and equipment	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing a process to support data file management activities.
	【To save data outside the etc. of healthcare institutions via networks】	(1) Grip of versions and continuity of data formats and transport protocols	Google is certified to the ISO27001 Standard, which regulates "Logging and Monitoring" (ISO 27001:2013, Annex A.12.4). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Integrity checks are in place at the application level and file system level to ensure data integrity.

MIC "Security Management Guidelines for Cloud Service Providers Handling Medical Information version1"			Google Response (EN)
Item No		Guideline	
		(1) Measures should be taken to prevent deterioration of equipments of the organization that accepts network or external storage.	Google is certified to the ISO27001 Standard, which regulates "Logging and Monitoring" (ISO 27001:2013, Annex A.12.4). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Integrity checks are in place at the application level and file system level to ensure data integrity.
		(1) Ensuring compatibility of network and external storage facilities	Google is certified to the ISO27001 Standard, which regulates "Logging and Monitoring" (ISO 27001:2013, Annex A.12.4). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Integrity checks are in place at the application level and file system level to ensure data integrity.
3.3.6	(A)	① The following information should be provided in response to a request from a medical institution or the like at the time of contract relating to the provision of services. ・Circumstance of development of basic policies and handling rules related to safety grip of medical-information, etc. ・Circumstance of Implementation of Implementation Systems for Safety grip of Medical Information, etc. ・Soundness of management based on creditworthiness and financial statements related to personal data safety grip based on actual results, etc...	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.3.6	(B)1	① It should be the minimum necessary to browse the commissioned medical information for maintenance and operation. ② Except in emergencies, if it is necessary to browse the system, the system shall be approved in advance and after by the system grip operator. ③ When the commissioned medical information is browsed in an emergency, the extent of the commissioned medical information and the reason why the commissioned medical information must be browsed in an emergency are indicated and approved by the systems grip operator. ④ Based on the Service Specification Adaptation Disclosure Form, agree on the scope and procedures of the browsing in (1) to (3) with medical institutions, etc. In addition, when medical information is browsed according to (ii) and (iii), a report to that effect is promptly sent to medical institutions.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
3.3.6	(B)2	① In order to prevent unauthorized access to medical information commissioned when performing scheduled maintenance and operations, measures such as setting authority should be taken. ② Take actions (encryption of databases, etc.) to ensure that systems grip personnel, operation personnel, maintenance personnel, etc. do not perform unintended browsing.	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.3.6	(C)1	① The analysis and analysis of entrusted medical information is not performed except when entrusted by medical institutions based on contract independent of contract for service provision. ② The information obtained by anonymously processing the entrusted medical information is also handled according to the medical information.	N/A
3.3.6	(C)2	① Submitted medical information shall not be provided to third parties, including the patient, except by law or on the basis of instructions from medical institutions. ② Include the contents of (1) in the contract related to service provision. ③ When third-party provide (browsing) of trusted medical information is made based on instructions from medical institutions, countermeasures as shown in 3.2.3 and 3.2.9 should be taken to prevent access and acquisition by persons other than those authorized by medical institutions. ④ In the case of providing (browsing) by a third party, the ID of the person who can browse and acquire and the authority to use should be promptly changed and deleted on the basis of the instructions of the medical institution or the person who has received the consignment (medical information collaboration network, etc.). ⑤ When a third party is provided with medical information entrusted based on instructions from medical institutions, the contents (provider (viewer), browsing information, browsing date and time, etc.) shall be reported to medical institutions. ⑥ Based on the service specification conformance disclosure document, agree with medical institutions on terms and ranges for providing third parties and reporting on the basis of steps (1) to (5).	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.3.7	(A)	① Agree personal data safeguards with medical institutions based on the service-specification conformance disclosures.	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.3.7	(B)	① Based on the Service Specifications Adaptation Document, the medical institution agrees on the provision of data required for explanations on external storage of personal data, etc. to be performed by medical institutions, etc., and the extent and role-sharing of the data with the medical institutions, etc. on the basis of the Service Specifications Adaptation Disclosure Document.	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.4.1		① When a part or all of the service is stopped or the service is changed (minor version upgrades are not included), measures are taken to minimize the impact on the medical institutions using the service, and notification is made with a sufficient period for the medical institutions to respond. ② Return the entrusted medical information to medical institutions in case of (1). The range of data to be returned (data type, period, etc.), data format (data item, item details, file format), return method, and condition are agreed with medical institutions based on the service specification conformance disclosure document. When the contents of the Service Specification Adaptation Disclosure Document are changed after the start of service use by medical institutions or other institutions, countermeasures are taken in accordance with (1). ③ Regarding the return of data in (2), it shall be carried out in accordance with Version 5 "Interoperability and standardize of information" of the MHLW Guidelines, and the contents thereof will be agreed with medical institutions, etc. Incidentally, since the data to be returned may include data obtained by lossy compression (image data, etc.) or conversion (password, etc.) performed by the cloud service provider, this fact is also agreed with medical institutions, etc. on the basis of the service specification compliance disclosure document. ④ When some or all of the services including the service change are stopped (minor version upgrades are not included) in (1), the contents of the response to the medical institution, etc. (except for the response to (2) in the transition support, etc.) and conditions are agreed with the medical institution, etc. based on the service specification conformance disclosure document. ⑤ When the use of services of medical institutions is terminated due to medical institutions or other reasons, the countermeasures shown in (2) and (3) should be taken. ⑥ When the service provision is stopped or the use of the service is stopped at a medical institution or the like, the recording is deleted, the medium is discarded, and the like promptly. When a record is deleted or a medium is discarded, data certifying the deletion should be submitted to medical institutions. ⑦ When keeping records to the minimum extent required in connection with support to medical institutions (including providing information to administrative authorities), agree with medical institutions on the objectives, scope, period, grip methods of records, safety grip actions, contact information, etc. based on the Service Specifications Adaptation Document. ⑧ The procedures for items (1) to (7) shall be included in the Operation grip Rules, etc.	Google is certified to the ISO27001 Standards, which regulates "Operational Procedures and Responsibilities" (ISO 27001:2013, Annex A.12.1) and "Network Security" (ISO 27001:2013, Annex A.13.1). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. System changes that may affect security, availability, processing integrity, or confidentiality are communicated to management and users who will be affected.

MIC "Security Management Guidelines for Cloud Service Providers Handling Medical Information version1"			Google Response (EN)
Item No		Guideline	
3.5.2		① When the online medical care system is connected to the medical information system, the requirements of 3.2 to 3.4 in this guideline are also applied to the cloud service provider that provides the online medical care system. ② The functions of the on-line medical system used in the patient terminal must not include the function of connecting to the medical information system during the on-line medical care, and agree with medical institutions etc. to provide information on this based on the service specification conformance disclosure document. ③ The division of responsibility between the cloud service provider and the patient providing an online medical treatment system used by a doctor is agreed with a medical institution or the like based on the service specification compliance disclosure statement.	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.6.1		① For PHR service providers, the requirements listed in 3.2.1 to 3.2.9 and 3.3.6 to 3.3.7 should be replaced as follows.・"Medical information" → "Medical information used by PHR 31"・"Medical Institutions"→"Patients, etc."・Cloud Service Provider→PHR Service Provider ② For PHR-service providers, the parts of the requirements in 3.2.9(2)(2)(1) that state that "TLS settings are appropriate to the highest level of security defined in the SSL/TLS Encryption Setting Guidelines" for both servers and clients should be read as "TLS settings should be limited to 1.2, server certificates issued by trusted authorities should be used, and identity verification should be carried out with certainty." For PHR-service providers, the number of PHR-service providers should be limited to 1.2, and PHR-service providers should be limited to the highest level of security specified in the SSL/TLS Encryption Setting Guidelines for both servers and clients. ③ PHR service providers shall delete the part stated in 3.2.3(2)(a)(iv)(iii)(3) "The MHLW Guidelines stipulate that "C. Minimum Guidelines for Two-Factor Certification" shall be adopted about 10 years after the publication of the 5th edition of MHLW Guidelines (May 2017). Therefore, they shall be able to respond to these requirements from time to time" in 3.2.3(2)(a)(iii). ④ For PHR service providers, "including the patient" in the requirements of 3.3.6(2)(c)(2)(i) shall be deleted. ⑤ For PHR service providers, the requirements listed in 3.6.3 are excluded from the requirements listed in 3.2.1 to 3.2.9 and 3.3.6 to 3.3.7. ⑥ When providing PHR services, establish procedures including the following and confirm that the procedures are followed.・Identification (confirmation of existence) of the patient or the like who is the ID applicant at the principal of registration・Authentication of patient when using (identification of user)・Principal newly received medical information with the ID of the patient (confirmation of the subject's identity) ⑦ For PHR service providers, among the requirements shown in 3.2.1 to 3.2.9 and 3.3.6 to 3.3.7, the requirements that result in "agreement with patient, etc. based on service specification conformance disclosure document" after the replacement in the above item (1) are excluded from the scope of application, and the following actions shall be taken instead of those requirements.・Develop operational grip regulations on how to obtain consent from subjects for personal data handled by PHR-services. The Managements grip Rules should include compliance with this Guideline to handle personal data.・Agree beforehand with the patient regarding the extent, method, and conditions of the return of medical information on the patient at the end of the PHR service or at the end of contract.・When medical institutions send medical information (grip by themselves) to PHR service providers to which the patient subscribes in response to an instruction from the patient, the responsibilities between the PHR service providers and the medical institutions are indicated in advance to the patient.・In agreeing with the patents on the provision of PHR-services, disclaimers and other matters should be defined in view of the fact that this information is a personal data protection legal consideration personal data and may be subject to the application of consumer protection laws and other measures.	N/A
3.6.2	(1)(A)	Establish a responsibility person responsible for grip the provision of services. ② Establish a responsibility person (system grip person) who is responsible for the grip of the information system and who has adequate technical skills and experiences in this information system. ③ Establish a responsible person for supervising operations related to the operation of information systems related to the provision of services. ④ Develop rules for designation and dismissal of responsible persons listed in (1) to (3).	Google is certified to the ISO27001 Standard, which regulates "Information Security Policy" (ISO 27001:2013, Annex A.5) and Organization of Information Security (ISO27001:2013, Annex A.6). Information security oversight and management controls, including documentation of information security policies are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
3.6.2	(1)(B)1	① Include information on services and confidentiality obligations on commissioned information in service provision contracts. The contract shall include the inclusion of a penalty for PHR service providers that violate confidentiality obligations and the contents of the patient's oversight to the treatment of the commissioned information.	Google is certified to the ISO27001 Standard, which regulates "Ownership of assets " (ISO 27001:2013, Annex A.7.1.2), Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Google's confidentiality and privacy policies.
3.6.2	(1)(B)2	① Clear that the contract for providing services complies with the content of the operation grip regulations and other latest related laws and regulations set forth in the following section (c) 1. and that safety grip actions should be implemented.	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.6.2	(1)(C)1	① Executive clarifies its personal data policies, privacy policies, etc. ② The guidelines for (1) include the implementation of safety grip actions specified in the guidelines of the personal data Protection Act and the personal data Protection Committee. ③ The guidelines for (1) include handling information not covered by the personal data Protection Act (information related to dead persons, etc.) in accordance with the personal data Protection Act because of the special nature of medical information used in PHRs. ④ Develop information security policies such as basic policies on information security and operational grip regulations. ⑤ Establish and document an organizational system that ensures compliance with information security policies.	Google is certified to the ISO27001 Standard, which regulates "Information Security Policy" (ISO 27001:2013, Annex A.5) and Organization of Information Security (ISO27001:2013, Annex A.6). Information security oversight and management controls, including documentation of information security policies are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
3.6.2	(1)(C)2	① Clarify the system for providing services, including emergency response.	Google is certified to the ISO27001 Standard, which regulates "Information Security Policy" (ISO 27001:2013, Annex A.5) and Organization of Information Security (ISO27001:2013, Annex A.6). Information security oversight and management controls, including documentation of information security policies are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
3.6.2	(1)(C)4	① Analyze the risk related to the service and decide to take necessary measures.	Google is certified to the ISO27001 Standard, which regulates "Information security reviews" (ISO 27001:2013, Annex A.18.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google performs risk assessments as required to support its ISMS.

MIC "Security Management Guidelines for Cloud Service Providers Handling Medical Information version1"			Google Response (EN)
Item No		Guideline	
3.6.2	(1)(C)5	① Document of grip methods of equipments, etc. ② Determine whether or not to confirm the location of the equipment, etc. by ledger grip, etc.	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001:2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
3.6.2	(1)(C)6	① Develop operational rules for grip of media on which personal data is recorded.	Google is certified to the ISO27001 Standard, which regulates "Documented Operating Procedures" (ISO27001:2013, Annex A.12.1.1). Google maintains robust internal documentation and maintains an ISMS, per ISO27001 requirements. All documentation in on systems that are replicated and subject to backup. Customers using Google Cloud Platform, retain all rights and responsibilities to configure and manage their environment, including development of operational guidance.
3.6.2	(1)(C)8	① Cluster the policies and content of audits on information systems, organizational systems, operations, etc. that provide services. ② In the case of using cloud services provided by third parties, clarify the policies and content of auditing or alternatives to the cloud services. ③ Record auditing practices and clarify how to preserve and grip such records.	Google is certified to the ISO27001 Standard, which regulates "Information Systems Audit Considerations" (ISO 27001:2013, Annex A.12.7), Information security oversight and management controls, including the establishment of internal audit oversight are reviewed and verified by a third party auditor for Google's SOC 2, Type II report
3.6.2	(1)(C)9	② Even when a service is provided using a cloud service provided by a third party contracted by the company, inquiry desks from the patient and the like are unified.	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.6.2	(1)(D)1	① Develop access grip rules that include the gathering and storage of records of access rights, accounts grip, authentication, and access to information systems by PHRs, and periodic reviews of the operational status of the access grip. ② Develop access grip rules that include preservation of access records related to the provision of services (including external access, user access, etc.), and periodic reviews and improvements of records.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
3.6.2	(1)(D)2	① Include the following in the contract regarding the treatment of medical information used in PHR. ・Grip the personal data as appropriate, distinguishing it from other types of information. ・Clarify that medical information used in PHRs should be handled according to personal data for information on dead people.	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.6.2	(2)(A)1	① Locking grip shall be performed for security boundaries such as installation locations of equipments, media, etc. used for services. ② Locking grip shall be performed for racks, etc. that store servers, etc. to be used for services. ③ Locking grip for cabinets that store media used for services	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0

MIC "Security Management Guidelines for Cloud Service Providers Handling Medical Information version1"			Google Response (EN)
Item No		Guideline	
3.6.2	(2)(A)2	① Restrict installation of equipments and media for services so that only authorized persons can enter and leave. ② Grip of access to equipment and media for services (including reviewing access records) is performed periodically. ③ Grip to enter and leave security boundaries, such as where equipments and media are installed, should be controlled by individual identification systems to identify people who enter and leave the service. When it is difficult to do so, measures are taken to identify the person entering or leaving, for example, changing the personal identification number or the like necessary for entering or leaving on a weekly basis. ④ In order to find out whether or not an unknown person enters or leaves the installation location of the equipment or media used for the service, the user is obliged to wear a name bid or the like. ⑤ Restrict the bringing in of personal properties irrelevant to the performance of services to the installation locations of equipments and media used for services. ⑥ Information that allows identification of the type of information handled, the function of the system, and the like should not be seen from the outside of the storage location (including rack and storage) of the equipment and media used for the service. ⑦ Items (1) to (6) shall be stipulated in the Operational grip Rules, etc.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0
3.6.2	(2)(A)3	① The facilities for physically preserving the equipment and media used for the service shall be installed in buildings that have functions and structures that can withstand disasters (earthquakes, water damage, thunder, fires, etc. and associated power outages) and that take measures against disaster failures (crippling, etc.).	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
3.6.2	(2)(A)4	① To prevent unauthorized access to buildings and rooms in which devices used for services are stored, security cameras and automatic intrusion monitoring devices should be installed. ② Monitoring images of security cameras and the like shall be recorded, grip shall be performed with a fixed period limit, and measures shall be taken to allow for post-referencing as needed. ③ Install surveillance cameras or the like in locations where equipments, media, and the like used for services are physically stored, store the records, and check the status to confirm that there are no unauthorized entrances and exits.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0
3.6.2	(2)(B)1	① In order to prevent peeping while the personal data is displayed, measures should be taken, such as pasting sheets of countermeasures against peeping on the operation terminal. ② Take measures so that the screen in operation does not fall within the field of view of anyone other than the operator.	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A.11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers
3.6.2	(2)(C)1	① The equipment and media in which personal data is physically stored must be the minimum required for the provision and operation of services, and the location and inventory of the equipment and media must be periodically checked. ② Attach anti-theft chains to significant equipments, such as PCs, where the personal data resides. ③ Provide that the personal data to be consigned is not stored in the terminal used for operation and maintenance in the operation grip regulations of the company, etc.	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001:2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.

MIC "Security Management Guidelines for Cloud Service Providers Handling Medical Information version1"			Google Response (EN)
Item No		Guideline	
3.6.2	(3)(A)1	① Issue accounts so that users of information systems can be identified and identified. (The ID is not shared by a plurality of users, except for the ID (non interactive ID) used by the information systems to use other information systems.) ② Authentication is performed to prevent user spoofing and the like. ③ Users include those who use services in patient-related areas, those who work in the operation or development of information systems, and those who have grip authorities, as well as those who use services in patient-related areas. ④ Issue of IDs to persons who are engaged in the operation or development of information systems or who have grip authorities is required to be minimized, and the information systems should be periodically inventoried.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001: 2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
3.6.2	(3)(A)2	① When a combination of a user ID and a password is used to identify and authentication an individual, measures are taken to keep the user ID and the password known only to the individual. Specifically, the following measures are taken. ・When an initial password is issued to a user, access to the information system is prohibited unless the password is changed at the time of initial use. ・The password other than the initial password is set by the user himself/herself, and is limited to the content which can be known only by the user himself/herself. ・When a password is set, a plurality of character types (alphanumeric characters, uppercase letters, lowercase letters, symbols, etc.) are used, and a rule is made up of character strings or the like having a sufficiently secure length, such as eight characters or more. ② Actions are taken to realize the following rules related to password authentication. ・A certain refractory time is set for re-entry when password entry is unsuccessful. ・When the number of failed password re-entries exceeds a certain number, re-entry is not accepted for a certain period of time. ③ A valid period that satisfies sufficient security is set for the password. However, when the user is a patient or the like, not only is the user particularly prompted not to use the password used in another service, but the service provider does not request the patient or the like to change the password periodically. ④ Even in the case where the authentication is not based on the ID and the password, the security equivalent to or more than that described above is ensured.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001: 2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Users are required to authenticate using valid credentials prior to resetting their password. Passwords are managed in accordance with a set of password construction, protection and management guidelines, which enforce the following: a) Minimum length b) Complexity c) History d) Idle time lockout setting Password security requirements are stipulated in the security guidelines and controls (password complexity, expiration, etc.) are built into systems to help ensure that Google password standards are enforced.
3.6.2	(3)(A)3	① The passwords of the users are encrypted for grip, for example, by storing the passwords using hashes. ② When introducing products that provide services, not only are the initial passwords changed, but the initial passwords are also stocked in the accounts, and unnecessary initial passwords are deleted. ③ When the user forgets the ID and password, the user is notified or reissued according to a procedure (including identification) prepared in advance. ④ When information such as passwords is leaked (including by hit from an unauthorized third party), the IDs are immediately invalidated, and new log-in information is reissued based on pre-established procedures to promptly notify the user. ⑤ When there is a fear of leakage of information such as a password, a measure is taken so that the password can be invalidated and changed after the fact is notified to the user himself/herself. ⑥ For passwords set by users, quality standards including content that is hard to be easily estimated by third parties shall be formulated, and operations shall be carried out based on these standards. ⑦ Perform grip of user passwords to ensure the security of passwords that cannot be set when changing passwords.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001: 2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
3.6.2	(3)(A)4	① Authentication related to the use of an information system by a person engaged in the operation or development of the information system or a person having the grip person authority is performed by a method having an authentication strength of two or more factor authentication. ③ When an authentication method using a fixed ID and password is adopted for user authentication, an effort is made to provide a function that can cope with adoption of an authentication method that does not rely solely on a fixed ID and password. ④ Alternative means and procedures for temporarily authenticating when some physical medium, physical information or the like is required for user authentication even if there is no exceptionally such medium or the like shall be defined in advance. ⑤ In the case where the alternative means and procedure are used, the difference in risk from the case of the original user authentication method is minimized. ⑥ Records are made to enable later tracing even when information systems are used by alternative methods and procedures, and this is grip.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001: 2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Users are required to authenticate using valid credentials prior to resetting their password. Passwords are managed in accordance with a set of password construction, protection and management guidelines, which enforce the following: a) Minimum length b) Complexity c) History d) Idle time lockout setting Password security requirements are stipulated in the security guidelines and controls (password complexity, expiration, etc.) are built into systems to help ensure that Google password standards are enforced.
3.6.2	(3)(B)1	① Actions should be taken to classify medical information used in PHR and other information. ② For medical information used in PHR, access control should be performed according to the information classification. ③ When providing services with resources using virtualization technologies, measures are taken to ensure that section grip can be performed logically.	N/A
3.6.2	(3)(B)3	① Services include the ability to grip medical-information used by entrusted PHRs on a patient-by-patient basis.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001: 2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
3.6.2	(3)(D)1	⑥ Regarding records of access by persons engaged in the operation or development of information systems or persons having grip authority, periodic reviews are made to ensure that there is no unauthorized access, etc.	Google is certified to the ISO27001 Standard, which regulates ""Access Control"" (ISO 27001: 2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Monitoring tools send automated alerts to operational personnel based on predetermined criteria. Incidents are escalated per policy.

MIC "Security Management Guidelines for Cloud Service Providers Handling Medical Information version1"			Google Response (EN)
Item No		Guideline	
3.6.2	(3)(D)2	① Restrict access to the resource in which the access record is stored to prevent unauthorized access. ② Ensure adequate space for storage of access records and ensure availability and integrity access records. ③ Actions are taken to prevent tampering, such as encrypting access records or periodically recording them on non-recordable media.	Google is certified to the ISO27001 Standard, which regulates "Cryptography" (ISO 27001:2013, Annex A.10) Customer data that is uploaded or created is encrypted at rest. We use several layers of encryption to protect customer data; adding redundant data protection and allowing us to select the optimal approach based on application requirements. Google publishes details about encryption and key management options for its Google Cloud Platform and G Suite products. To read more about key management and encryption, please see: https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including development of appropriate encryption measures.
3.6.2	(3)(D)3	① In order to ensure the reliability of the time of the access record, synchronization between the time of the information system and the standard time or equivalent time information provided by the trusted authority is performed daily or more frequently.	Google is certified to the ISO27001 Standard, which regulates ""Access Control"" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Monitoring tools send automated alerts to operational personnel based on predetermined criteria. Incidents are escalated per policy.
3.6.2	(3)(E)1	① The Operation grip Regulations and other regulations specify that measures are to be taken to prevent clearing screens, etc. on the operation and maintenance terminals, etc. of services. ② A surveillance camera or the like is used to appropriately monitor the area where the service operation and maintenance terminal or the like is installed. ④ In order to reduce the risk of hijacking a terminal or a session, a session for which a certain interruption time has elapsed after the user logs on can be blocked or forcibly logged off.	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A.11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers
3.6.2	(3)(F)1	① When constructing an information system, establish procedures to prevent viruses, malware, etc. from being mixed, and construct the system in accordance with the procedures. ② The pattern definition file of the anti-virus software is always updated to the latest one. ③ When building an information system, if it is necessary to bring in or download a program from an external medium, implementation the latest anti-virus software in advance. In addition, the latest security patch is applied in consideration of the degree of influence on the information system. ④ In cases where service usage environments are subject to hit by viruses, etc., the impact of service provision is promptly made known to the subject, etc., and the required measures, etc. are sought. ⑤ Information on information systems vulnerabilities is acquired from information sources such as the JPCERT Coordination Center (JPCERT/CC), the Cabinet Cyber Security Center (NISC), and the Institute for Information Processing of Independent Administrative Organizations (IPA) periodically and when needed, and confirmed.	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001:2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/.
3.6.2	(3)(F)2	① When connecting an external network to a device that stores medical information used in PHR, a security gateway (a firewall, a router, or the like installed at the boundary of the network) is installed, and access control of each network interface is performed based on established policies such as limitation of a connection destination, limitation of a connection time, and the like. ② An intrusion detection system (IDS), an intrusion prevention system (IPS), or the like is introduced at the boundary of a connection network with a patient or the like to detect an unauthorized event on the network, or to block unauthorized traffic. ③ The intrusion detection system or the like updates the signature and detection rules and applies security patches to the software so that the intrusion detection system or the like can cope with the latest hit and unauthorized accesses at all times. ④ When a device cannot be installed at a network boundary, such as when hosting is used, the same control is performed in each information processing apparatus.	Google has implemented network and host base tools to detect and respond to potential security incidents. Google maintains automated log collection and analysis tools to support investigations.
3.6.2	(3)(H)2	① Obtain a backup of the information system based on the results of the risk analysis performed in 3.2.1(2)(c)4.①. Determine what backups should be obtained, how often they should be obtained, how often they should be stored, how they should be grip, etc. and include the details in the Operation grip Rules, etc. ② Regarding the backups obtained according to (1), perform periodic checks required for the grip methods of the recording medium to confirm that the recorded content is not tampered with or destroyed. ③ For the backup to be stored in the recording medium, the backup content, the use starting date, and the use ending date are clarified based on the characteristics of the medium (tape/disk, capacity, etc.), and the grip is made. ④ When the end date of use of the backup recording medium as the target is approaching, the contents thereof are copied to another medium or the like before the end date. ⑤ Include the procedures in (1) to (4) in the operation grip regulations, etc. and provide the required training to employees and subcontractors.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing a process to support data file management activities.
3.6.2	(3)(I)1	① A configuration diagram of equipment and software in an information system is created. ② Create a network configuration diagram of the information system. ③ Prepare documents with descriptions of system requirements for the devices included in the configuration diagrams created in (1) and (2). ④ Documentations relating to the specifications of updates and the like of the equipment, software, and the like constituting the information system and the update history thereof are prepared.	For Google Cloud Platform related installation, configutation and use of products, services, and features, please refer to: https://cloud.google.com/docs/ For G Suite related installation, configutation and use of products, services, and features, please refer to: https://gsuite.google.com/learning-center/
3.6.2	(1)(C)3	① Create important documents, such as basic policies on information security and operation grip regulations, and formulate regulations on grip, and grip the documents based on these. ② Appropriate documentation of the operation of services and resource grip shall be provided for grip as security-related information.	Google is certified to the ISO27001 Standard, which regulates "Documented Operating Procedures" (ISO27001:2013, Annex A.12.1.1). Google maintains robust internal documentation and maintains an ISMS, per ISO27001 requirements. All documentation in on systems that are replicated and subject to backup. Customers using Google Cloud Platform, retain all rights and responsibilities to configure and manage their environment, including development of operational guidance.

MIC "Security Management Guidelines for Cloud Service Providers Handling Medical Information version1"			Google Response (EN)
Item No		Guideline	
3.6.2	(3)(I)2	① Include the measures and procedures related to the quality grip of the equipment and software used for services in the operation grip regulations, etc. ② Educations employees about the quality grip of equipment and software used for services. ③ Request the service-related consignee to respond to the quality-of-service grip required by its own company to meet the requirements of the main guideline. ④ Include the content, procedures, etc. of internal audits related to system configuration and software operation status in the operation grip regulations, etc.	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001:2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
3.6.2	(4)(A) 1	① For personnel (employees, dispatchers, etc.) engaged in the provision of services, the content of confidentiality obligations should be included in employment contracts or dispatch contracts, or should be included in work rules, etc.	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google. com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.6.2	(4)(A) 2	① Education and train personnel involved in providing services on personal data policy and personal data safety grip. ② This education and training is performed at the beginning of work and periodically after work.	Google is certified to the ISO27001 Standard, which regulates "Information Security Awareness, Education and Training" (ISO 27001:2013, Annex A.7.2.2), Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All Google contractors undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new contractors agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.
3.6.2	(4)(A) 3	① Confidentiality obligations related to personal data handled during work should be included in employment contracts or dispatch contracts or included in work rules, etc. when personnel engaged in the provision of services leave the office. ② For the personal data where the personnel involved in the provision of the services had grip in the work, request return at the time of departure (including internal change), and confirm that the systems grip personnel were returned. ③ The confidentiality obligations of personnel involved in the provision of the service at the time of retirement or after the end of contract shall be included in the education and training in section 2 above.	Google is certified to the ISO27001 Standard, which regulates "Ownership of assets " (ISO 27001:2013, Annex A.7.1.2), Hiring practices controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report.
3.6.2	(4)(A) 4	① Include appropriate penalties in employment contracts or dispatch contracts or in work rules, etc. for employees, dispatch operators, etc. who violate the above-mentioned 1-3.	Google is certified to the ISO27001 Standard, which regulates "Ownership of assets " (ISO 27001:2013, Annex A.7.1.2), Hiring practices controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report.
3.6.2	(4)(B) 1	② The subcontractor is required to comply with the same personal data guidelines as its own. ③ Include confidentiality obligations related to the consignment operation in the contract related to the re-consignment. ④ Confirm with the subcontractor that the subcontractor personnel has the same confidentiality obligation as that of the company. ⑤ Confirm that the subcontractor has taken the safety grip measures specified in this guideline.	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google. com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.6.2	(5)(A) 2	① The operational grip rules are as follows: ・The necessity of providing services should be periodically checked for the personal data to be grip or the medium in which it is stored. ・The procedures for discarding the personal data and the medium in which it is stored, which are not required for the provision of services. ・When discarding the personal data which is not necessary for providing services and the medium in which it is stored, actions are taken to prevent the subject from suffering unexpected damage (for example, notifying the discarding standard in advance).	Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" (ISO 27001: 2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" (ISO 27001:2013,Annex A. 11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.
3.6.2	(6)(A) 1	① When a person engaged in maintenance of an information system and a person having grip authority accesses the information system for the purpose of the task, the access is performed by a accounts issued for each person. ② The tasks performed by the accounts specified in (1) are logged and saved so that the accessed personal data can be identified.	Google is certified to the ISO27001 Standard, which regulates ""Access Control"" (ISO 27001: 2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Monitoring tools send automated alerts to operational personnel based on predetermined criteria. Incidents are escalated per policy.
3.6.2	(6)(A) 2	① Persons engaged in the maintenance of information systems and those with grip authorities shall strictly grip information systems so as not to leak accounts for business use.	Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Google's confidentiality and privacy policies.
3.6.2	(6)(B) 1	① Prepare procedures for maintenance operations by remote maintenance, and take safety grip actions to prevent unauthorized access to data systems. ② Records of maintenance work by remote maintenance are obtained by access logs, etc., and the systems grip person confirms the content promptly.	Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development, and Maintenance" (ISO27001:2013, Annex A.14). Information security oversight and management controls, including software development controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud Platform retain all right and responsibilities to configure and manage their environment, including developing a process to support input management acitivities.
3.6.2	(6)(B) 2	① Records and grip the results of operations performed in the maintenance of information systems using operation logs and the like. ② The status of medical information used in the accessed PHR is reviewed using the obtained operation log and the like.	Google is certified to the ISO27001 Standard, which regulates ""Access Control"" (ISO 27001: 2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Monitoring tools send automated alerts to operational personnel based on predetermined criteria. Incidents are escalated per policy.
3.6.2	(6)(C) 1	① When checking the operation of information systems, data for testing should be used instead of data including personal data accepted in principle. ② Procedures including confirmation of operations by personnel and consignees for whom confidentiality obligations as shown in 3.2.4 are imposed should be defined when data including consigned personal data is inevitably used for confirmation of operations of information systems.	Google is certified to the ISO27001 Standard, which regulates ""Access Control"" (ISO 27001: 2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Monitoring tools send automated alerts to operational personnel based on predetermined criteria. Incidents are escalated per policy.

MIC "Security Management Guidelines for Cloud Service Providers Handling Medical Information version1"			Google Response (EN)
Item No		Guideline	
3.6.2	(6)(C) 2	① When it is necessary to bring a device or the like storing medical information to be used in PHR outside the organization of a patient or PHR service provider (including a subcontractor) for the purpose of maintenance (for example, repair of the device), the procedure should be formulated.	Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" ((ISO 27001:2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" ((ISO 27001:2013,Annex A.11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.
3.6.2	(7)(A) 1	① Policies and rules related to the removal (including removal from the consignor) of equipments and media that store information related to services (consignment information, information related to information systems, etc.) shall be defined in the Operation grip Rules. ② The term "take-out" in (i) includes not only physical taking-out but also send to the outside through a network.	Google is certified to the ISO27001 Standard, which regulates "Documented Operating Procedures" (ISO27001:2013, Annex A.12.1.1). Google maintains robust internal documentation and maintains an ISMS, per ISO27001 requirements. All documentation in on systems that are replicated and subject to backup. Customers using Google Cloud Platform, retain all rights and responsibilities to configure and manage their environment, including development of operational guidance.
3.6.2	(7)(A) 2	① For recording media and recording equipment used for services, include the following in the Operation grip Rules.・Grip System and grip Methods・Treatment of Recording Media and Recording Devices・Policies and rules related to the removal (including removal from the consignor) of equipments and media that store information related to services (consignment information, information related to information systems, etc.) (In addition to physical removal, "removal" includes transmission to the outside via a network).・When information on services is taken out, the equipment and media that store the information are stolen or lost (in addition to physical theft or loss of equipment and media at the time of take-out, system grip is sent to the outside that is not approved by the system operator (including malicious responses by third parties, erroneous transmissions by employees, etc.))・Connection conditions for connecting to external networks, safety grip actions, etc. (Specific measures to prevent leakage or tampering of stored data (anti-malware measures, encryption, implementation of firewalls, etc.)	Google is certified to the ISO27001 Standard, which regulates "Documented Operating Procedures" (ISO27001:2013, Annex A.12.1.1). Google maintains robust internal documentation and maintains an ISMS, per ISO27001 requirements. All documentation in on systems that are replicated and subject to backup. Customers using Google Cloud Platform, retain all rights and responsibilities to configure and manage their environment, including development of operational guidance.
3.6.2	(7)(A) 3	① Education employees about the contents described in "2. Response to Recording Media and Recording Equipments for Services". ② Compliance with the above operation grip regulations is also required for the subcontractor.	Google is certified to the ISO27001 Standard, which regulates "Information Security Awareness, Education and Training" (ISO 27001:2013, Annex A.7.2.2), Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All Google contractors undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new contractors agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.
3.6.2	(7)(B)	① For devices and media that store information on services, perform register grip, etc. and periodically check the location of the devices and media.	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001:2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
3.6.2	(7)(C) 1	① Set a startup password for a device or the like used for a service. ② Measures should be taken to prevent an unauthorized activation of a device by a third party, such as setting an activation password that is hard to guess and periodically changing the activation password according to the characteristics of the device. ③ A plurality of authentication elements are combined for login and access to an information device that stores information related to a service.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Users are required to authenticate using valid credentials prior to resetting their password. Passwords are managed in accordance with a set of password construction, protection and management guidelines, which enforce the following: a) Minimum length b) Complexity c) History d) Idle time lockout setting Password security requirements are stipulated in the security guidelines and controls (password complexity, expiration, etc.) are built into systems to help ensure that Google password standards are enforced.
3.6.2	(7)(C) 2	① Procedures for taking out equipments, media, etc. that store information related to services include such things as applying encryption measures to the devices, media itself, applying encryption measures to the stored information, and setting passwords.	Google is certified to the ISO27001 Standard, which regulates "Cryptography" (ISO 27001:2013, Annex A.10) Customer data that is uploaded or created is encrypted at rest. We use several layers of encryption to protect customer data; adding redundant data protection and allowing us to select the optimal approach based on application requirements. Google publishes details about encryption and key management options for its Google Cloud Platform and G Suite products. To read more about key management and encryption, please see: https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including development of appropriate encryption measures.
3.6.2	(7)(C) 3	① When a device storing information on a service is taken out, a minimum number of applications necessary for the purpose of taking out the device are installed. ② Determine the procedure for installing an application when a device that stores information related to a service is taken out.	N/A
3.6.2	(7)(C) 5	① In business, when a mobile terminal storing information on a service is taken out, connection to a public wireless LAN is not performed.	N/A

MIC "Security Management Guidelines for Cloud Service Providers Handling Medical Information version1"			Google Response (EN)
Item No		Guideline	
3.6.2	(8)(B) 1	① Develop BCP and contention plans for services. ② The BCP and contention plan formulated in (1) should include the contents of emergency systems and service recovery procedures.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
3.6.2	(8)(B) 3	① Take actions to preserve logs and other records required for investigating the causes of problems in the provision of services due to cyber hit, etc. ② In case (1), the status of failures occurring in the service and the prospects for recovery should be promptly reported to the patient, etc.	Google is certified to the ISO27001 Standard, which regulates "Information Security Policy" (ISO 27001:2013, Annex A.5) and Organization of Information Security (ISO27001:2013, Annex A.6). Information security oversight and management controls, including documentation of information security policies are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.
3.6.2	(8)(B) 4	① To ensure that the results of data processing performed in an emergency do not conflict after service restoration, measures should be taken to ensure the consistency of the data (e.g., stipulation of rules and verification methods).	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and G Suite customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
3.6.2	(9)(A) 1	① In the network, measures necessary to protect information from eavesdropping, tampering, communication through wrong routes, destruction, and the like (maintenance of implementation standards and procedures of information exchange, encryption of communication, and the like) are performed. ② Take necessary measures (implementation of a server certificate, etc.) to prevent access destination spoofing (session hijacking, phishing, etc.).	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001:2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/.
3.6.2	(9)(A) 3	① Network devices, such as routers, select security targets or similar documents defined in the ISO15408 that conform to this guideline.	Google is certified to the ISO27001 Standard, which regulates "Documented Operating Procedures" (ISO27001:2013, Annex A.12.1.1). Google maintains robust internal documentation and maintains an ISMS, per ISO27001 requirements. All documentation in on systems that are replicated and subject to backup. Customers using Google Cloud Platform, retain all rights and responsibilities to configure and manage their environment, including development of operational guidance.
3.6.2	(9)(A) 4	① Security measures against the information itself, such as encryption, are implemented between the transmission source and the transmission destination. ② When the SSL/TLS is used in providing services, actions corresponding to TLS1. 2 should be taken.	Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. Please see https://cloud.google.com/security/encryption-in-transit/ for more informaiton.
3.6.2	(9)(A) 5	① When connecting via an open network using the HTTPS, the setting of the TLS is limited to 1.2, a server certificate issued by a trusted authority is used, and the identity of the server is reliably confirmed. ② SSL-VPN is not used in principle. ③ In providing services, when connecting by software-based IPsec or TLS1. 2, appropriate measures should be taken for hit caused by looping between sessions (accessing closed sessions that are not legitimate routes).	Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. Please see https://cloud.google.com/security/encryption-in-transit/ for more informaiton.
3.6.2	(9)(B)	① When maintenance is performed by remote maintenance, appropriate safety grip actions such as setting up access points, restricting protocols, and access authority grip should be taken as needed.	Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development, and Maintenance" (ISO27001:2013, Annex A.14). Information security oversight and management controls, including software development controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud Platform retain all right and responsibilities to configure and manage their environment, including developing a process to support input management acitivities.
3.6.2	(10)(B) 1	① Minimize the necessary to browse medical information used in commissioned PHRs for maintenance and operation. ② Except in emergencies, if it is necessary to browse the system, the system shall be approved in advance and after by the system grip operator. ③ When medical information used in commissioned PHRs is browsed in an emergency, the extent of the commissioned information and the reason why the commissioned information needs to be browsed in an emergency are indicated and approved by the systems grip operator.	N/A

MIC "Security Management Guidelines for Cloud Service Providers Handling Medical Information version1"			Google Response (EN)
Item No		Guideline	
3.6.2	(10)(B) 2	① In order to prevent unauthorized access to medical information used in a commissioned PHR when performing scheduled maintenance and operations, measures such as setting authority should be taken. ② Take actions (encryption of databases, etc.) to ensure that systems grip personnel, operation personnel, maintenance personnel, etc. do not perform unintended browsing.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001: 2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
3.6.2	(10)(C) 2	① Medical information used in commissioned PHRs shall not be provided to third parties except in law cases or on the basis of patient instructions. ② Include the contents of (1) in the contract related to service provision. ③ When third-party provide (browsing) of medical information used in commissioned PHRs is performed based on instructions from the patient, countermeasures as shown in 3.2.3 and 3.2.9 should be taken so that persons other than those authorized by the patient cannot browse and acquire the medical information. ④ When third-party provisioning (browsing) is performed in accordance with (ii), measures shall be taken to quickly change and delete the ID and authority of a person who can browse and acquire the information based on instructions from the patient or the person who has been entrusted with it (medical information collaboration network, etc.). ⑤ When a third party is provided with medical information to be used in a commissioned PHR based on instructions from a patient or the like, the contents (provider (viewer), browsing information, browsing date and time, etc.) should be reported to the patient or the like.	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA: https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/