US Food & Drug Administration (FDA) - 21 CFR Part 11

Google Cloud Mapping

This document is designed to help regulated customers supervised by the US FDA (“**regulated entity**”) to consider 21 CFR Part 11 /eCFR (“**framework**”) in the context of Google Cloud.

We focus on the electronic records & electronic signatures (ERES) requirements of the framework: §11.30 Controls for Open Systems*, §11.50 Signature manifestations, §11.70 Signature/record linking, §11.100 General requirements, §11.200 Electronic signature components and controls, §11.300 Controls for identification codes/passwords, §820.22 Quality audit, §820.25 Personnel, §820.40 Document controls, §820.100 Corrective and preventive action and §820.22 Quality audit. For each paragraph, we provide commentary to help you understand how you can address the requirements using the Google Cloud services and the Google Cloud Compliance Reports and Certificates.

NOTE:
*§11.10 Controls for Closed Systems is deemed not applicable since systems hosted in the cloud cannot be considered closed systems. However; the same §11.10 controls and control references are applicable to “Open Systems”.
**Google Responsibilities vs Customer Responsibilities - Google Cloud is responsible for controls for the Google Cloud services and customers retain ownership and control of the systems/workloads they set-up on Google Cloud, in alignment with the Google Cloud Shared Responsibility model in the Google Cloud Security Foundations whitepaper.

#	Framework reference	**Google	**Customer	Google Cloud commentary	Google Cloud Compliance Reports / Certificates reference
1	**§11.30 Controls for open systems.** Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in §11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality. Ref. §11.10(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	☑	☑	**Change Management:** Google has a robust change management process and security policy that is documented and requires approvals from relevant stakeholders before being released into production. Google maintains policy and procedures to ensure consideration of security, quality and availability throughout the SDLC (Software Development Lifecycle). Every Google Cloud product maintains a well documented release and deployment process. This process is validated for each product during the semi-annual compliance audit cycle. **Configuration Management (Infrastructure Qualification):** Google’s infrastructure is designed and purpose built for Google. Baseline configuration settings are defined for infrastructure components and Google maintains configuration management tools to detect and correct deviations from its security baselines and collects and secures audit records. Our configuration management controls are audited as part of our third party audit certifications and attestation reports. **Logging:** Google maintains an automated log collection and analysis tool to review and analyse log events. Customers retain control and ownership over change, configuration and log management to their systems hosted on Google Cloud.	CSA CCM v4: CCC-01, CCC-02, CCC-03, CCC-04, CCC-05, CCC-06, CCC-07, CCC-08, CCC-09, LOG-01, LOG-02, LOG-03, LOG-04, LOG-05, LOG-07, LOG-08, LOG-09, LOG-10, LOG-14 SOC 2 Type II: CC7.4, CC6.2 ISO 27001: A.12.1.4, 8.1* (partial) A.14.2.2, 8.1* (partial) A.14.2.3, A.12.1.2, A.12.4, A.12.4.1, A.12.4.2, A.12.4.3, A.12.6.1, A.12.6.2, A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7, A.9.2.3, A.9.4.4, A.9.4.1, A.18.2.3, A.18.1.3 ISO 27017: CLD12.1.5, 14.1.1, 14.2.1, 15.1.1, 15.1.3, 12.1.2, 12.4, 12.4.1, 12.4.3, 12.6.1, 15.1.1, 15.1.3, 16.1.1, 16.1.2, 16.1.7, 9.2.3, 9.4.4, 9.4.1,18.1.3, CLD.9.5.1 , CLD12.4.5 ISO 27018: 9.2.3, 9.4.1, 9.4.4, 12.4.1 , 12.4.2, 12.4.3 , 16.1.2 , 16.1.7 , 18.2.3, 18.1.3 NIST SP800-53 R3: CA-1, CA-6, CA-7, CM-2, CM-3, CM-5, CM-6, CM-9, PL-2, PL-5, SI-2, SI-6, SI-7, AU-1, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-9, AU-11, AU-12, AU-14, SI-4 BSI C5:2020: BEI01, BEI02, BEI03, BEI04, BEI05, BEI06, BEI07

US Food & Drug Administration (FDA) - 21 CFR Part 11

Google Cloud Mapping

2	**§11.30 Controls for open systems.** Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in §11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality. Ref. §11.10(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.	☑	☑	Customers do not need Google's assistance to port their data. Google will enable you to access and export your data throughout the duration of our contract. You can export your data from the Services in a number of industry standard formats (e.g. .doc, .xls, .pdf, logs, and flat files). Google offers solutions to support customers in data export and migration such as: • Google Kubernetes Engine is a managed, production-ready environment that allows portability across different clouds as well as on premises environments. • Migrate to Containers allows you to move and convert workloads directly into containers in Google Kubernetes Engine. • You can export/import an entire VM image in the form of a .tar archive. Find more information on images and on storage options. Google provides documentation regarding how customers may port data. Our GDPR resource site provides an entry point for information regarding portability and interoperability of data. Further, Google Cloud storage and database solutions offer fine-grained IAM permissions to control which employees can export data. In addition, Google Cloud implements limitations, such as preventing the export of BigQuery tables to raw files or Google Sheets, the inability to export more than 1GB of table data, the inability to export data from multiple tables all at once, and others.	CSA CCM v4: IPY-01, IPY-02, IPY-04, IPY-05 SOC 2 Type II: None ISO 27001: 6.1.1, 6.1.1(e)(2), 6.1.2, 6.1.2(a)(1), 6.1.2(a)(2), 6.1.2(b), 6.1.2 (c), 6.1.2(c)(1), 6.1.2(c)(2), 6.1.2(d), 6.1.2(d)(1), 6.1.2(d)(2), 6.1.2(d)(3), 6.1.2(e), 6.1.2(e)(1), 6.1.2(e)(2), 6.1.3, 6.1.3(a), 6.1.3(b), 8.1, 8.3, 9.3(a), 9.3(b), 9.3(b)(f), 9.3(c), 9.3(c)(1), 9.3(c)(2), 9.3(c)(3), 9.3(d), 9.3(e), 9.3(f), A.14.2.3, A.12.6.1, A.18.1.1, A.18.2.2, A.18.2.3 ISO 27017: 12.6.1, 18.1.1 ISO 27018: None NIST SP800-53 R3: SC-8, SC-8(1) BSI C5:2020: IPI-02, IPI-04, IPI-05
3	**§11.30 Controls for open systems.** Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in §11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality. Ref. §11.10(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	☑	☑	Policies and procedures are established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness. Customers retain control and ownership over their content. Customers are responsible for managing their data retention policies. Customers may leverage the features of our storage services. Please see product documentation for examples of such services: • Google Cloud online storage products • Retention policies and retention policy locks	CSA CCM v4: DSP-18, LOG-09 SOC 2 Type II: A1.2, A1.3, I3.21 ISO 27001: 9.2(g), 7.5.3(b), 5.2 (c), 7.5.3(d), 5.3(a), 5.3(b), 8.1, 8.3, A.12.3.1, A.8.2.3 ISO 27017: 12.3.1, 15.1.1, 15.1.3 ISO 27018: None NIST SP800-53 R3: CP-2, CP-6, CP-7, CP-8, CP-9, SI-12, AU-11 BSI C5:2020: RB-06, RB-08
4	**§11.30 Controls for open systems.** Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the	☑	☑	Customers retain control and ownership over identity & access management to their systems hosted on Google Cloud. Customers can customize access to data by organization and user and assign administrative access profiles based on roles. Google provides customers with solutions which help to prevent	CSA CCM v4: IAM-01, IAM-02, IAM-03, IAM-04, IAM-05, IAM-06, IAM-07 SOC 2 Type II: CC5.1, CC7.4, CC3.1, CC3.3, CC5.3

	confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in §11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality. Ref. §11.10(d) Limiting system access to authorized individuals.			unauthorized access by controlling access rights and roles for Google Cloud resources and to implement more granular control over access. For example: • Cloud Identity and Access Management • Identity-Aware Proxy - identity and context to guard access to your applications and VMs. • BeyondCorp - a zero trust solution that enables secure access with integrated threat and data protection. • Access Transparency - enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location). • Cloud Logging - fully managed service that performs at scale and can ingest application and system log data, as well as custom log data from GKE environments, VMs, and Google Cloud services. Cloud Logging allows you to analyze selected logs and accelerate application troubleshooting. • Cloud Monitoring - provides visibility into the performance, uptime, and overall health of cloud-powered applications. Google's internal data access policies and processes are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process your data. access rights and levels are based on their job function and role. Google restricts access based on need-to-know and job function in accordance with applicable legal and compliance requirements. Google provides (under NDA) customers with a SOC 2 report that includes testing of Google's access controls. For more information, refer to Trusting your data with Google Cloud whitepaper. In the Cloud Data Processing Addendum, Google makes commitments to protect your data, including regarding access control and privilege management.	ISO 27001: A.9.1.1, A.9.2.1, A.9.2.2, A.9.2.5, A.9.1.2, A.9.4.1, A.13.1.1, A.9.4.4,, A.9.2, A.9.2.3, A.9.2.4, A.6.1.2, 5.2(c), 5.3(a), 5.3(b), 7.5.3(b), 7.5.3(d), 8.1, 8.3, 9.2(g), A.9.4.5, A.18.1.3, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 ISO 27017: 9.2.1, 9.2.2, 9.1.2, 9.4.1, 9.4.4, 9.2, 9.2.3, 9.2.4, 18.1.3, CLD12.4.5 ISO 27018: 9.2, 9.2.1, 9.2.2, 9.2.3, 9.2.4, 9.2.5, 9.2.6, 9.4.5, 18.1.3, 9.1.1, 9.3.1, 9.4.1, 9.4.2, 9.4.3, 9.4.4 NIST SP800-53 R3: AC-1, IA-1, AU-9, AU-11, AU-14, CM-7, MA-3, MA-4, MA-5, AC-2, AC-5, AC-6, AU-1, AU-6, SI-1, SI-4, CM-5, CM-6, CA-3, RA-3, AC-3, IA-2, IA-4, IA-5, IA-8, PS-6, SA-7, SI-9, PM-10, PS-6, PS-7, PS-4, PS-5, , AC-11, AU-2, IA-6, SC-10, SC-3, SC-19 BSI C5:2020: RB-13, IDM-01, IDM-06, IDM-07, IDM-08, IDM-03, IDM-02, IDM-13, DLL-01, SPN-03, IDM-05, IDM-04, IDM-12
5	**§11.30 Controls for open systems.** Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in §11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality. Ref. §11.10(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator	☑	☑	Google maintains an automated log collection and analysis tool to review and analyze log events. Google restricts physical and logical access to audit logs. Google Cloud retains Google-generated customer data access audit logs for no longer than 30 days. It is the customer's responsibility to offload these audit log records from the Google Cloud Console and manage the retention of logs. Customers that have longer audit log retention requirements can export logs to Cloud Storage, BigQuery, or Cloud Pub Sub to stream log entries to other applications or repositories. Customers are also responsible for the retention of audit records for customer applications within Google Cloud. Admin Activity audit logs are retained by Google for 400 days. Admin Activity logs contain log entries for API calls or other administrative actions that modify the configuration or metadata of resources.	CSA CCM v4: LOG-01, LOG-02, LOG-03, LOG-04, LOG-05, LOG-06, LOG-07, LOG-08, LOG-09, LOG-10, LOG-11, LOG-12, LOG-13, LOG-14 SOC 2 Type II: CC6.2 ISO 27001: A.12.4.1, A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.3, A.12.4.1, A.9.2.3, A.9.4.4, A.9.4.1, A.16.1.2, A.16.1.7, A.18.2.3, A.18.1.3 ISO 27017: 12.4.1, 12.4.1, 12.4.3, 12.4.3, 12.4.1, 9.2.3, 9.4.4, 9.4.1, 15.1.1, 15.1.3, 16.1.2, 16.1.7, 18.1.3, CLD.9.5.1 , CLD12.4.5

	entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying			For example, the logs record when VM instances and App Engine applications are created and when permissions are changed. Customers retain control and ownership over identity & access management to their systems hosted on Google Cloud including audit trails and logging management.	ISO 27018: 9.2.3, 9.4.1, 9.4.4, 12.4.1 , 12.4.2, 12.4.3 , 16.1.2 , 16.1.7 , 18.2.3, 18.1.3 NIST SP800-53 R3: AU-1, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-9, AU-11, AU-12, AU-14, SI-4 BSI C5:2020: RB-10, RB-13, RB-14
6	**§11.30 Controls for open systems.** Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in §11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality. Ref. §11.10(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	☐	☑	Customers retain control and ownership over operational system checks to enforce permitted sequencing of steps and events, as appropriate.	N/A
7	**§11.30 Controls for open systems.** Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in §11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality. Ref. §11.10(g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	☑	☑	Customers retain control and ownership over identity & access management to their systems hosted on Google Cloud. Customers can customize access to data by organization and user and assign administrative access profiles based on roles. Google provides customers with solutions which helps to prevent unauthorized access by controlling access rights and roles for Google Cloud resources and to implement more granular control over access. For example: • Cloud Identity and Access Management • Identity-Aware Proxy - identity and context to guard access to your applications and VMs. • BeyondCorp - a zero trust solution that enables secure access with integrated threat and data protection. • Access Transparency - enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location). • Cloud Logging - fully managed service that performs at scale and can ingest application and system log data, as well as custom log data from GKE environments, VMs, and Google Cloud services. Cloud Logging allows you to analyze selected logs and accelerate application troubleshooting. • Cloud Monitoring - provides visibility into the performance, uptime, and overall health of cloud-powered applications.	CSA CCM v4: IAM-01, IAM-02, IAM-03, IAM-04, IAM-05, IAM-06, IAM-07 SOC 2 Type II: CC5.1, CC7.4, CC3.1, CC3.3, CC5.3 ISO 27001: A.9.1.1, A.9.2.1, A.9.2.2, A.9.2.5, A.9.1.2, A.9.4.1, A.13.1.1, A.9.4.4,, A.9.2, A.9.2.3, A.9.2.4, A.6.1.2, 5.2(c), 5.3(a), 5.3(b), 7.5.3(b), 7.5.3(d), 8.1, 8.3, 9.2(g), A.9.4.5, A.18.1.3, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 ISO 27017: 9.2.1, 9.2.2, 9.1.2, 9.4.1, 9.4.4, 9.2, 9.2.3, 9.2.4, 18.1.3, CLD12.4.5 ISO 27018:9.2, 9.2.1, 9.2.2, 9.2.3, 9.2.4, 9.2.5, 9.2.6, 9.4.5, 18.1.3, 9.1.1, 9.3.1, 9.4.1, 9.4.2, 9.4.3, 9.4.4 NIST SP800-53 R3: AC-1, IA-1, AU-9, AU-11, AU-14, CM-7, MA-3, MA-4, MA-5, AC-2, AC-5, AC-6, AU-1, AU-6, SI-1, SI-4, CM-5, CM-6, CA-3, RA-3, AC-3, IA-2, IA-4, IA-5, IA-8, PS-6, SA-7, SI-9, PM-10,

US Food & Drug Administration (FDA) - 21 CFR Part 11

Google Cloud Mapping

				Google's internal data access policies and processes are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process your data. access rights and levels are based on their job function and role. Google restricts access based on need-to-know and job function in accordance with applicable legal and compliance requirements. Google provides (under NDA) customers with a SOC 2 report that includes testing of Google's access controls. For more information, refer to Trusting your data with Google Cloud whitepaper. In the Cloud Data Processing Addendum, Google makes commitments to protect your data, including regarding access control and privilege management.	PS-6, PS-7, PS-4, PS-5, , AC-11, AU-2, IA-6, SC-10, SC-3, SC-19 BSI C5:2020:RB-13, IDM-01, IDM-06, IDM-07, IDM-08, IDM-03, IDM-02, IDM-13, DLL-01, SPN-03, IDM-05, IDM-04, IDM-12
8	**§11.30 Controls for open systems.** Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in §11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality. Ref. §11.10(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	☑	☑	All user interfaces are designed with secure coding practices to prevent web attacks such as cross site scripting or other popular input based attacks. If a user attempts to input data that does not meet system parameters, the system will reject the input. Users will not be able to execute commands without correcting that input. Users can input information in the Google Cloud Console, however the user interface is designed to only allow responses that meet specific parameters that can be processed by Google Cloud. If a user inputs invalid data that isn't within the parameters the system automatically rejects the data. Customers retain control and ownership over ensuring that checks to determine, as appropriate, the validity of the source of data input or operational instruction are in place for the devices, systems and applications that they build and host on Google Cloud.	CSA CCM v4: AIS-03 SOC 2 Type II: PI1.2, PI1.3, PI1.5 ISO 27001: A.10.9.2, A.10.9.3, A.12.2.1, A.12.2.2, A.12.2.3, A.12.2.4, A.12.6.1, A.15.2.1 ISO 27017: None ISO 27018: None NIST SP800-53 R3: SI-10, SI-11, SI-2, SI-3, SI-4, SI-6, SI-7, SI-9 BSI C5:2020: None
9	**§11.30 Controls for open systems.** Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in §11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality. Ref. §11.10(i) Determination that persons who develop, maintain, or use electronic record / electronic signature systems have the education, training, and experience to perform their assigned tasks.	☑	☑	All Google employees undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new employees 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. Google maintains a robust and up-to-date Information Security Management System that is audited at least yearly and signed off by business leadership. As part of the ISO/IEC 27001 certified ISMS, roles and responsibilities are documented and authorized by leadership.	CSA CCM v4: HRS-10, HRS-11, HRS-12 SOC 2 Type II: CC2.2, CC2.3, CC5.5, CC5.6 ISO 27001: 7.2(a), 7.2(b), A.7.2.2, A.11.1.5, A.9.3.1, A.11.2.8, A.11.2.9 ISO 27017: 7.2.2 ISO 27018: None NIST SP800-53 R3: AT-1, AT-2, AT-3, AT-4, AC-11, MP-2, MP-3, MP-4 BSI C5:2020: HR-03

US Food & Drug Administration (FDA) - 21 CFR Part 11

Google Cloud Mapping

				Customers retain control and ownership over training of their personnel including maintaining appropriate sign-offs and records.	
10	**§11.30 Controls for open systems.** Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in §11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality. Ref. §11.10(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	☐	☑	Customers retain control and ownership over the establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	N/A
11	**§11.30 Controls for open systems.** Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in §11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality. Ref. §11.10(k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	☑	☑	Google has established and maintains policies and procedures over security and privacy of its systems and personnel. Google reviews its security and privacy policies at least annually. Google's cross functional security policy team meets periodically throughout the year to address emerging issues and risk and issue new or amend existing policies or guidelines, as needed. Our internal documentation platform uses a source control management system to manage changes to policies and procedures and retains an audit trail of these changes. Customers retain control and ownership over the establishment of relevant systems documentation including revisions and change control of documentation.	CSA CCM v4: GRC-01, GRC-03, GRC-04 SOC 2 Type II: CC3.2 ISO 27001: 8.1, A.5.1.2 ISO 27017: 15.1.1, 15.1.3, 18.1.2 ISO 27018: None NIST SP800-53 R3: AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IA-5, IR-1, MA-1, MP-1, PE-1, PL-1, PM-1, PS-1, RA-1, SA-1, SC-1, SI-1 BSI C5:2020: OIS-07
12	**§11.50 Signature manifestations.** (a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: (1) The printed name of the signer; (2) The date and time when the signature was executed; and	☐	☑	Customers retain control and ownership over the establishment of, and adherence to digital/electronic signature management.	N/A

	(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.				
13	**§11.70 Signature/record linking.** Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.	☐	☑	Customers retain control and ownership over the establishment of, and adherence to digital/electronic signature management.	N/A
14	**§11.100 General requirements.** (a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else. (b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual. (c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system,used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures. (1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC–100), 5600 Fishers Lane, Rockville, MD 20857. (2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.	☐	☑	Customers retain control and ownership over the establishment of, and adherence to digital/electronic signature management.	N/A
15	**§11.200 Electronic signature components and controls.** (a) Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password. (i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. (ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components. (2) Be used only by their genuine owners; and,	☐	☑	Customers retain control and ownership over the establishment of, and adherence to digital/electronic signature management.	N/A

	(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals. (b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.				
16	**§11.300 Controls for identification codes/passwords.** Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include: (a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password. (b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging). (c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls. (d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management. (e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.	☐	☑	Customers retain control and ownership over the establishment of, and adherence to digital/electronic signature management.	N/A
17	**§820.22 Quality audit** Each manufacturer shall establish procedures for quality audits and conduct such audits to assure that the quality system is in compliance with the established quality system requirements and to determine the effectiveness of the quality system. Quality audits shall be conducted by individuals who do not have direct responsibility for the matters being audited. Corrective action(s), including a re-audit of deficient matters, shall be taken when necessary. A report of the results of each quality audit, and reaudit(s) where taken, shall be made and such reports shall be reviewed by management having	☑	☑	Google has a robust compliance program, designed to meet emerging requirements from our customers and regulators. We work with regulators, government bodies, and third-party auditors globally to comply with regional, country or industry specific requirements. Google undergoes a number of independent third party audits and internal audits on a regular basis to verify and provide assurance of our security, privacy and compliance controls. Our certifications include many internationally accepted independent quality, security and privacy standards including ISO/IEC9001, CSA STAR, HITRUST CSF, ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SOC 1/2/3 and NIST 800-53.	CSA CCM v4: A&A-02, A&A-04 SOC 2 Type II: CC3.2, CC1.2, CC2.3, CC4.1 ISO 27001: 4.3, 5, 4.4, 4.2(b), 6.1.2(a)(1), 6.2, 6.2(a), 6.2(d), 7.1, 7.4, 9.3, 10.2, 7.2(a), 7.2(b), 7.2(c), 7.2(d), 7.3(b), 7.3(c), A5.1.1, A.7.2.2, 18.2.1, 4.3(a), 4.3(b), 5.1(e), 5.1(f), 9.1, 9.2, 9.3(f) ISO 27017: 5.1.1, 7.2.2, 15.1.1, 15.1.3, 18.1.2 ISO 27018: None

	responsibility for the matters audited. The dates and results of quality audits and re-audits shall be documented.			Google Cloud also supports compliance with industry and country specific regulations (such as PCI DSS) and we continue to expand our list of certifications to assist our customers with their compliance obligations, including the “right to audit” Google Cloud. For more information on our compliance, visit the Compliance Resource Center and Compliance Reports Manager to download reports and certifications. Google maintains a public website that details all current compliance, regulatory, and privacy standards Google either complies or aligns with. Customers retain control and ownership over their QMS, including procedures for quality audits and conduct such audits to assure that the quality system is in compliance with the established quality system requirements and to determine the effectiveness of the quality system. Quality audits shall be conducted by individuals who do not have direct responsibility for the matters being audited. Corrective action(s), including a re-audit of deficient matters, shall be taken when necessary. A report of the results of each quality audit, and reaudit(s) where taken, shall be made and such reports shall be reviewed by management having responsibility for the matters audited. The dates and results of quality audits and re-audits shall be documented.	NIST SP800-53 R3: AC-1, AT-1, AU-1, CA-1, CM-1, IA-1, IR-1, MA-1, MP-1, MP-1, PE-1, PL-1, PS-1, SA-1, SC-1, SI-1, CA-2, CA-6 , RA-5 BSI C5:2020: SA-01, COM-03
18	**§820.25 Personnel** (a) General. Each manufacturer shall have sufficient personnel with the necessary education, background, training, and experience to assure that all activities required by this part are correctly performed. (b) Training. Each manufacturer shall establish procedures for identifying training needs and ensure that all personnel are trained to adequately perform their assigned responsibilities. Training shall be documented. (1) As part of their training, personnel shall be made aware of device defects which may occur from the improper performance of their specific jobs. (2) Personnel who perform verification and validation activities shall be made aware of defects and errors that may be encountered as part of their job functions.	☑	☑	Google provides role-specific privacy and security training. The training is administered online and completion is tracked. Privacy and security training are required annually. Google maintains a robust and up-to-date Information Security Management System that is audited at least yearly and signed off by business leadership. As part of the ISO/IEC 27001 certified ISMS, roles and responsibilities are documented and authorized by leadership. Customers retain control and ownership over training of their personnel including maintaining appropriate sign-offs and records.	CSA CCM v4: HRS-10, HRS-11, HRS-12 SOC 2 Type II: CC2.2, CC2.3, CC5.5, CC5.6 ISO 27001: 7.2(a), 7.2(b), A.7.2.2, A.11.1.5, A.9.3.1, A.11.2.8, A.11.2.9 ISO 27017: 7.2.2 ISO 27018: None NIST SP800-53 R3: AT-1, AT-2, AT-3, AT-4, AC-11, MP-2, MP-3, MP-4 BSI C5:2020: HR-03
19	**§820.40 Document controls** Each manufacturer shall establish and maintain procedures to control all documents that are required by this part. The procedures shall provide for the following: (a) Document approval and distribution. Each manufacturer shall designate an individual(s) to review for adequacy and approve prior to	☑	☑	Google has established and maintains policies and procedures over security and privacy of its systems and personnel. Google reviews its security and privacy policies at least annually. Google's cross functional security policy team meets periodically throughout the year to address emerging issues and risk and issue new or amend existing policies or guidelines, as needed. Our internal documentation platform uses a source control management system to manage changes to policies and procedures and retains an audit trail of these changes.	CSA CCM v4: GRC-01, GRC-03, GRC-04 SOC 2 Type II: CC3.2 ISO 27001: 8.1, A.5.1.2 ISO 27017: 15.1.1, 15.1.3, 18.1.2

	issuance all documents established to meet the requirements of this part. The approval, including the date and signature of the individual(s) approving the document, shall be documented. Documents established to meet the requirements of this part shall be available at all locations for which they are designated, used, or otherwise necessary, and all obsolete documents shall be promptly removed from all points of use or otherwise prevented from unintended use. (b) Document changes. Changes to documents shall be reviewed and approved by an individual(s) in the same function or organization that performed the original review and approval, unless specifically designated otherwise. Approved changes shall be communicated to the appropriate personnel in a timely manner. Each manufacturer shall maintain records of changes to documents. Change records shall include a description of the change, identification of the affected documents, the signature of the approving individual(s), the approval date, and when the change becomes effective.			Customers retain control and ownership over the establishment of relevant systems documentation including revisions and change control of documentation.	ISO 27018: None NIST SP800-53 R3: AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IA-5, IR-1, MA-1, MP-1, PE-1, PL-1, PM-1, PS-1, RA-1, SA-1, SC-1, SI-1 BSI C5:2020: OIS-07
20	**§820.100 Corrective and preventive action** (a) Each manufacturer shall establish and maintain procedures for implementing corrective and preventive action. The procedures shall include requirements for: (1) Analyzing processes, work operations, concessions, quality audit reports, quality records, service records, complaints, returned product, and other sources of quality data to identify existing and potential causes of nonconforming product, or other quality problems. Appropriate statistical methodology shall be employed where necessary to detect recurring quality problems; (2) Investigating the cause of nonconformities relating to product, processes, and the quality system; (3) Identifying the action(s) needed to correct and prevent recurrence of nonconforming product and other quality problems; (4) Verifying or validating the corrective and preventive action to ensure that such action is effective and does not adversely affect the finished device; (5) Implementing and recording changes in methods and procedures needed to correct and prevent identified quality problems; (6) Ensuring that information related to quality problems or nonconforming product is disseminated to those directly responsible for assuring the quality of such product or the prevention of such problems; and (7) Submitting relevant information on identified quality problems, as well as corrective and preventive actions, for management review.	☑	☑	Google has 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. Google's security incident management program is structured around the NIST guidance on handling incidents (NIST SP 800–61). 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. We outline Google's end-to-end data incident response process in our whitepaper. Further; Google has dedicated teams that coordinate the continual improvement and monitoring of the effectiveness, continuing suitability, and adequacy of the Information Security Management System (ISMS) through the use of information security policies, information security objectives, audit results, analysis of continuous monitoring events, corrective and preventive actions, and management review. At least annually, a qualified, independent entity conducts	CSA CCM v4: SEF-02, SEF-03, SEF-04, SEF-05, SEF-07, SEF-08 SOC 2 Type II: CC5.5, CC6.2 ISO 27001: 5.3 (a), 5.3 (b), 7.5.3(b), 5.2 (c), 7.5.3(d), 8.1, 8.3, 9.2(g), Annex, A.16.1.1, A.16.1.2 ISO 27017: 16.1.1, 16.1.2, 6.1.1, 7.2.2, CLD.6.3.1, CLD12.4.5 ISO 27018: 16.1.1 , 16.1.2, 16.1.2.3 NIST SP800-53 R3: IR-1, IR-2, IR-3, IR-4, IR-5, IR-7, IR-8, SI-4, SI-5 BSI C5:2020: SIM-05, SIM-06, SIM-07

	(b) All activities required under this section, and their results, shall be documented.			testing of Google's ISMS to determine whether the ISMS conforms to the identified information security requirements and are effectively implemented, maintained, performed as expected, and are continually improved upon. This process is also verified as part of our ISO9001 Quality Management System (QMS) certification. Customers retain control and ownership over the establishment and maintenance of procedures for implementing corrective and preventive action.	
22	**Data Center & Infrastructure Qualification.** Even if the regulated entity is not the owner of the data center (DC), it is responsible for the GxP data stored in those DCs which means the pharma company should qualify the data center. The external supplier providing the data center services should be assessed to ensure compliance with applicable regulatory and security requirements. External providers can demonstrate qualification through through showing that DC controls exist (access, availability, environmental) and are tested periodically: • certifications of data centers • physical inspection of data centers • qualification guides or SOC reports	☑	☑	**Data Center Qualification** 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, and 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. As you get closer to the data center floor, security measures also increase. Access to the data center floor is only possible via a security corridor which implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter. Less than one percent of Googlers will ever set foot in one of our data centers. **Configuration Management (Infrastructure Qualification)** Google's infrastructure is designed and purpose built for Google. Baseline configuration settings are defined for infrastructure components and Google maintains configuration management tools to detect and correct deviations from its security baselines and collects and secures audit records. Our configuration management controls are audited as part of our third party audit certifications and attestation reports. Google undergoes a number of independent third party audits and internal audits on a regular basis to verify and provide assurance of our security, privacy and compliance controls over our Data Center and infrastructure. Our certifications include many internationally accepted independent quality, security and privacy standards including ISO/IEC9001, CSA STAR, HITRUST CSF, ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SOC 1/2/3 and NIST 800-53. Google Cloud also supports compliance with industry and country specific regulations (such as PCI DSS) and we continue to expand our list of certifications to assist our customers with their compliance obligations, including the "right to audit" Google Cloud. For more information on our compliance, visit the Compliance Resource Center and Compliance Reports Manager to download reports and certifications. Google	CSA CCM v4: DCS-01, DCS-02, DCS-03, DCS-04, DCS-05, DCS-06, DCS-07, DCS-08, DCS-09, DCS-10, DCS-11, DCS.12 SOC 2 Type II: CC3.1, CC5.1, CC5.7 ISO 27001: A.8, A.11.1.1, A.11.2.6, A.11.2.7, A.8.1.1, A.8.1.2, A.11.1.2, A.11.1.6, A.11.2.5, 8.1 (partial) A.12.1.2, A.11.1.1 ISO 27017: 11.2.7, 8.1.1, 12.1.2, 15.1.1, 15.1.3 ISO 27018: 8 NIST SP800-53 R3: PE-8,IA-3, IA-4, AC-17,PE-1,PE-17, CM-8, PE-4, PE-5,PE-7, PE-16, MA-1, MA-2, PE-16, PE-2, PE-3, PE-6,PE-18 BSI C5:2020: AM-01, AM-02, AM-05, AM-01, KOS-01, AM-08, PS-05, AM-07, SA-01, SPN-02, SPN-03, PS-01, PS-02

				maintains a public website that details all current compliance, regulatory, and privacy standards Google either complies or aligns with. Customers retain control and ownership over the qualification of the infrastructure components that they set-up for their systems and workloads on Google Cloud.	