Google Cloud Whitepaper
May 2023

Google Cloud HIPAA overview guide

Google Cloud

Table of contents

Disclaimer

This whitepaper applies to Google Cloud products described at cloud.google.com. The content contained herein is current as of May 2023 and represents the status quo at publication. Google's security policies and systems may change going forward, as we continually improve protection for our customers. As an additional resource, please reference "HIPAA Compliance on Google Cloud" at https://cloud.google.com/security/compliance/hipaa.

Introduction

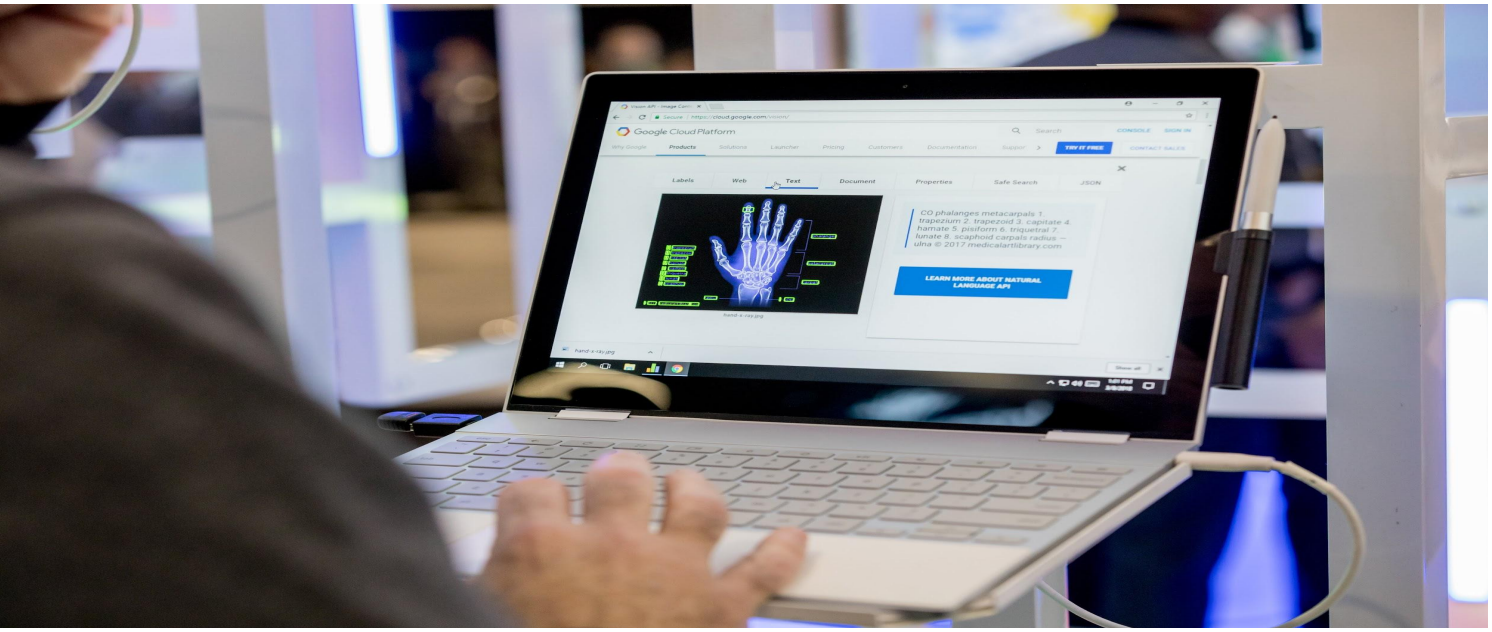
Many industries are becoming digital industries through software advances that are driving the explosive growth of digital services. These digital transformations provide an environment for app and infrastructure modernization, data democratization, people connections, and trusted transactions. Healthcare organizations are increasingly using cloud platforms to personalize patient care, analyze large datasets more effectively, enhance research and development collaboration, and share medical knowledge. Leveraging cloud platforms can also help healthcare organizations increase the privacy and security of information systems, and better comply with applicable laws and regulations while reducing the burden of compliance.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) set standards in the United States to protect individually identifiable health information. Since HIPAA's inception, there have been several updates including rules pertaining to privacy in 2003, security in 2005, enforcement in 2006, and breach notification in 2009. Also in 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act was signed into law and strengthened the civil and criminal enforcement of HIPAA rules. The US Department of Health and Human Services announced an omnibus rule in 2013 to a) modify the rules for privacy, security and enforcement and b) implement statutory amendments contained in the HITECH Act.

HIPAA applies to health plans, most healthcare providers, and healthcare clearinghouses - collectively known as "covered entities" - that manage protected health information (PHI) and to persons or entities that perform certain functions on their behalf, known as "business associates".

The HIPAA Privacy Rule requires covered entities and their business associates to safeguard the privacy of PHI handled in any medium, while the HIPAA Security Rule obligates them to protect the confidentiality, integrity, and availability of PHI they create, receive, maintain, or transmit electronically with administrative, physical, and technical measures. Covered entities and business associates also have breach notification obligations and duties.

As an industry-leading cloud service provider (CSP), Google Cloud Platform (GCP) offers tailored industry solutions and products to support HIPAA-compliant digital transformations. By choosing GCP, customers also leverage the innovation of the entire Google ecosystem to build fast, scale quickly, and optimize costs on the industry's most secure, trusted cloud.



GCP's administrative, physical, and technical controls also help healthcare organizations meet their privacy, security, and compliance objectives. Google is committed to protecting customers' information and undergoes routine audits by independent third parties to verify our compliance with numerous globally recognized security and data privacy standards. In fact, Forrester Research recognized Google Cloud as a Leader for Public Cloud Native Security for our security capabilities and features.

To learn about Google Cloud's innovative technologies that support HIPAA compliance, visit the Google Cloud HIPAA Compliance page, which has a current list of services covered by the GCP HIPAA Business Associate Agreement (BAA) products, and the Google Cloud Blog posts for Healthcare & Life Sciences.

This guide describes measures GCP takes to ensure our compliance with numerous globally recognized security and data privacy standards. It also explains how healthcare organizations can use GCP's products and services to meet HIPAA requirements. While references to — and details of — regulatory standards and guidance are provided as a framework for this discussion, these do not constitute legal advice for healthcare organizations nor for any other entities.

Google is committed to protecting customers' information and undergoes routine audits by independent third parties to verify our compliance with numerous globally recognized security and data privacy standards.

Overview of HIPAA

HIPAA is a federal law administered and enforced by the U.S. Department of Health & Human Services (HHS) that requires organizations to safeguard individuals' medical and health-related information. The law aims to support the secure maintenance and appropriate sharing of sensitive health data.

In this section we define some important terms, describe HIPAA rules, and outline the obligations that are applicable to certain organizations that handle individuals' medical and health-related information. We base the following information on Title 45 of the Code of Federal Regulations, Part 160 and Part 164, and the HHS' official guidance. To learn more, please refer to the links provided herein, as well as the HHS' FAQ section.

Topics covered in this section

Definitions of HIPAA key terms

To promote consistent understanding of HIPAA-related terms, we have included definitions in this section, per HHS guidance.

Protected Health Information

Protected health information (PHI) is "individually identifiable health information" but excludes individually identifiable information "in education records by the Family Educational Rights and Privacy act, as amended," in employment records held by a covered entity in its roles as employer; and regarding a person who has been deceased for more than 50 years. Additionally, records described in 20 U.S.C. 1232g(a)(4)(B)(iv) are not categorized as PHI. The individually identifiable health information a covered entity and its business associates create, receive, maintain, or transmit solely in electronic form is defined as "electronic protected health information" (ePHI).

Individually identifiable health information (IIHI) is a subset of health information, including demographic information collected from an individual, and:

- Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
- Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and
    - That identifies the individual; or
    - With respect to which there is a reasonable basis to believe the information can be used to identify the individual the provision of healthcare to the individual; or
    - The past, present, or future payment for the provision of healthcare to an individual

As an example, a medical record, laboratory report, or hospital bill could be PHI if one item contains information that identifies a patient (such as by name) and has medical and health-related information or payment data concerning that patient.

Covered entities

Under HIPAA, covered entities include the following:

Health plans

Individual and group plans that provide or pay the cost of medical care. Such plans include:

- Health, dental, vision, and prescription drug insurers
- Health maintenance organizations (HMOs)
- Medicare, Medicaid, and Medicare supplement insurers
- Long-term care insurers (excluding nursing home fixed-indemnity policies)
- Employer-sponsored group health plans multi-employer health plans
- Government and church-sponsored health plans

Healthcare providers

Healthcare providers that conduct certain financial and administrative transactions electronically for which HHS has adopted a standard. Such providers include:

- Doctors
- Clinics
- Psychologists
- Dentists
- Chiropractors
- Nursing homes
- Pharmacies

Healthcare clearinghouses

Entities that process non-standard health information they receive from another entity into a standard format, or conversely. Such entities might include:

- Billing services
- Repricing companies
- Community health management information systems

To learn more, refer to the HHS Covered Entities guidance. To help determine if you are a covered entity, refer to the HHS decision guidance tool that is maintained by the Centers for Medicare & Medicaid Services (CMS).

Business associate

A business associate is an individual or entity that performs certain functions or activities that involve the use or disclosure of PHI for a covered entity. Example business associate functions and activities include: claims processing or administration; data analysis, processing, or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing.

Business associates include a persons or entities that provide a covered entity with a wide variety of services including legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial.

Business associates must comply with HIPAA's Privacy, Security, and Breach Notification Rules. To learn more, refer to HHS' guidance on business associates.

Business associate agreement

The HIPAA Privacy Rule permits covered entities to disclose PHI to business associates as long as associates provide adequate written assurance that they will safeguard the PHI in line with the Privacy Rule. The business associate agreement (BAA) must include a number of requirements for business associates with respect to use, protection, retention, access, and other aspects of PHI.

For example, the BAA must:

- Establish the permitted and required uses and disclosures of PHI — and prohibit the business associate from using or further disclosing the PHI, other than as allowed by the written agreement or as mandated by law.

- Require the business associate to implement appropriate safeguards to prevent improper use or disclosure of the PHI. If any unauthorized use or disclosure occurs, the associate must notify the covered entity.
- Require the business associate to make internal practices, books, and records with respect to the use and disclosure of PHI available to HHS for evaluation of the covered entity's compliance with the HIPAA Privacy Rule.

Covered entities should be aware of the additional HIPAA responsibilities that they incur when entering into or executing a BAA. If a business associate suffers a material breach or violates HIPAA requirements, the covered entity may be required to take action. These actions may include steps to cure the breach, end the violation, or terminate the business arrangement.

To learn more, refer to the HHS Business Associate Contracts guidance.

Security incident

A security incident is the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with an information system.

Breach of PHI

A breach is the impermissible acquisition, access, use, or disclosure of PHI that compromises its security or privacy under the Privacy Rule. According to HHS, real-world examples of breaches include unauthorized access to an electronic medical record in a hospital or a hacking in a medical service's network server that results in unlawful disclosure of health-related records.

When such an event occurs, HIPAA regards it as a breach unless the covered entity or business associate establishes the probability of compromise is low based on a risk assessment that considers factors such as:

- Nature and extent of the PHI involved
- Unauthorized person or entity who used the PHI or to whom the PHI was disclosed
- Whether the PHI was actually obtained or viewed
- Extent to which the covered entity or business associate has mitigated the risk to the PHI

The HIPAA Privacy, Security, and Breach Notification Rules

To promote consistent understanding of HIPAA-related rules, we provide a brief overview in this section.

HIPAA's principal components concern the standards set by the Privacy, Security, and Breach Notification Rules, which govern the protection of PHI and ePHI. The HHS Office for Civil Rights has authority to enforce HIPAA rules. Covered entities and their business associates must comply with the following HIPAA rules by implementing adequate safeguards. The Privacy Rule grants individuals greater control over their PHI.

Privacy Rule

The Standards for Privacy of Individually Identifiable Health Information (the Privacy Rule) aims to safeguard the privacy of individuals and their PHI, while allowing appropriate uses and disclosures of the data without patients' approval to improve the healthcare system and overall public health. The Privacy Rule also gives individuals rights over their own PHI such as the rights to examine and gain a copy of their health records, request corrections, and direct a covered entity to transmit an electronic copy of their PHI to a third party.

Privacy Rule requirements for covered entities

Covered entities are required to:

- Implement reasonable and appropriate administrative, technical, and physical safeguards to protect the privacy of PHI they hold or transfer in any form or media against misuse.
- Implement policies and procedures to limit the use and disclosure of, and requests for, PHI to the minimum necessary to achieve an intended purpose. To learn more, refer to the HHS' guidance on the minimum necessary requirement and its HIPAA FAQs for Professionals that address disclosures.
- Give individuals notice of (1) how it may use and disclose their PHI; (2) their rights in regard to the PHI and how to exercise those rights; and (3) the entity's legal obligations under HIPAA. To learn more, refer to the HHS' guidance on notice.

De-identification of health information and patient rights

HHS recognizes how technological advances in various fields are accelerating research into positive healthcare outcomes and that this research often requires data sources that are extremely large, complex, and aggregated from multiple sources. De-identification is the process of removing identifiers from protected health information to mitigate the privacy risks

to individuals. Properly de-identified health information from a combination of sources presents immense opportunity for advanced research to support comparative effectiveness studies, policy assessments, life sciences research, and other beneficial endeavors. Covered entities or their business associates can use de-identified health information, such as anonymized patient data, for medical research without adhering to HIPAA requirements. For more information on de-identification of health information please refer here.

Except in some circumstances, individuals are granted certain rights in relation to their protected health information. This includes:

- The right to access their protected health information
- The right to have covered entities amend their protected health information in a designated record set when that information is inaccurate or incomplete
- Request the restriction of uses or disclosures of PHI
- Receive an accounting of disclosures of their PHI (within six years of the request)

To learn more, please refer to HHS' Privacy Rule guidance.

Security Rule

The Security Standards for the Protection of Electronic Protected Health Information (the Security Rule) seeks to ensure the Privacy Rule's protections through appropriate technical and non-technical measures. The Security Rule is designed "to protect the privacy of individuals' health information" while permitting covered entities to use technologies that enhance healthcare.

Unlike the Privacy Rule, the Security Rule applies only to protected health information in electronic form (i.e., ePHI) that covered entities and their business associates create, receive, maintain, or transmit. The Security Rule requires these organizations to implement reasonable and appropriate administrative, technical, and physical safeguards to:

- Ensure the confidentiality, integrity, and security of ePHI
- Defend against any reasonably anticipated threats to the integrity or security of ePHI
- Protect against any impermissible uses or disclosures of ePHI
- Ensure its workforce complies with the security standards

HIPAA requires covered entities or their business associates to implement the following administrative, physical, and technical safeguards for ePHI.

Administrative safeguards

- Security management processes that include risk analysis and management procedures such as mapping ePHI flows and audit log reviews
- A security official
- Workforce security to ensure proper access to ePHI, such as determining who has access to ePHI or the authority to decide who has such access
- Information access management policies consistent with the Privacy Rule, namely, restricting access to ePHI to those persons or entities that need such access
- Security awareness and training for employees, such as security reminders, password management, and log-in monitoring
- Security incident procedures, such as how to respond to, mitigate, and document suspicious pings on the network that come from an outside source
- Contingency plans, including data backup, disaster recovery, and emergency mode operation plans
- Regular and ongoing evaluations of the entity's policies and controls based on the Security Rule's required safeguards

To learn more, refer to the HHS guidance on administrative safeguards.

Physical safeguards

- Facility access and authorization controls such as locked doors, security cameras, and private security guard personnel
- Workstation security protections and use policies such as logging off of electronic systems after a certain period of time and regular antivirus software updates
- Device and media security controls such as the reuse or disposal of electronic media or hardware, including the clearing or purging (i.e., degaussing) ePHI from electronic media, or destroying the media (e.g., pulverizing or incinerating)

To learn more, refer to the HHS guidance on physical safeguards.

Technical safeguards

- User and software access controls, such as automatic logoff functions
- Authentication controls, including assigning a unique name and/or number to each workforce member, such as requiring a password or PIN, a token or key, or biometric information
- Audit controls
- Integrity controls to protect ePHI from improper alteration or destruction, such as digital signatures or checksum verification
- Transmission security of ePHI, such as encryption

To learn more, refer to the HHS guidance on technical safeguards.

For further details on the Security Rule, consult HHS' guidance on the Security Rule and cyber-related security issues. To find help for performing risk evaluations, consult the official HIPAA Security Risk Assessment Tool, the Guidance on Risk Analysis, and the Basics of Risk Analysis and Management.

Breach Notification Rule

In the event of a breach of "unsecured protected health information," the Breach Notification Rule requires covered entities to give notice to affected individuals, the HHS Secretary, and, in certain situations, the media. Unsecured protected health information is PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology stipulated by HHS guidance.

In addition, the business associate must notify the covered entity following a breach in regard to its own systems. The Breach Notification Rule also specifies the content, timing, and other requirements for incident reporting.

To learn more, refer to the HHS Breach Notification Rule guidance.

The cloud service provider as a business associate

Covered entities and their business associates may engage a cloud service provider (CSP) to store or process ePHI via a BAA. Cloud customers should understand that the HHS does not recognize a certification for HIPAA compliance and that complying with HIPAA is a shared responsibility between the customer and the CSP. In response to whether "CSPs offer HIPAA-compliant cloud services," HHS' Office for Civil Rights states that it "does not endorse, certify, or recommend specific technology or products."

Nonetheless, according to the HHS' Guidance on Cloud Computing, when a covered entity or its business associate uses a CSP to create, receive, maintain, or transmit ePHI on its behalf, HIPAA classifies the CSP as a business associate. Consequently, the covered entity and the CSP must enter into a HIPAA-compliant BAA that requires the CSP to safeguard the PHI, among other responsibilities. As a business associate, the CSP must comply with the HIPAA Privacy, Security, and Breach Notification Rules.

Customers that are subject to HIPAA and want to utilize any Google Cloud products in connection with PHI must review and accept Google's BAA. Google ensures that the Google products covered under our BAA meet HIPAA requirements and align with our ISO/IEC 27001, 27017, and 20718 certifications and SOC 2 report.

The Google Cloud BAA covers Google Cloud's entire infrastructure (all regions, all zones, all network paths, all points of presence) and services that can be found here.

GCP privacy, security, and compliance overview

Google Cloud provides comprehensive information privacy and security protections that enable our customer's HIPAA compliant solutions. We constantly work to expand our privacy and security capabilities. In this section, we describe the GCP information safeguards that are most relevant to HIPAA requirements and explain how we share compliance responsibilities with our customers under the Shared Responsibility Model.

Topics covered in this section

The Shared Responsibility Model

GCP-managed privacy safeguards

Privacy is fundamental to Google. We build privacy into our products from the earliest stages, and we continually evolve our practices. Google Cloud protects the privacy of our customers' information by providing them with meaningful privacy configuration options and maintaining and continually evolving our data security features. Google Cloud undergoes regular audits, maintains industry-accepted certifications, provides industry-standard contractual protections, and shares tools and information to help customers strengthen their enterprises' compliance abilities. To learn more, refer to the Google Cloud Privacy page and read about our Dedicated Privacy Team.

Our commitments to you about your data
Your data is critical to your business, and you take great care to keep it safe and under your control. We want you to feel confident that taking advantage of G Suite and Google Cloud Platform doesn't require you to compromise on security or control of your business's data.

At Google Cloud, we believe that trust is created through transparency, and we want to be transparent about our commitments and what you can expect when it comes to our shared responsibility for protecting and managing your data in the cloud.

When you use Google Cloud, you can:

1. **Know that your security comes first in everything we do.**

   We promptly notify you if we detect a breach of security that compromises your data.
2. **Control what happens to your data.**

   We process customer data according to your instructions. You can access it or take it out at any time.
3. **Know that customer data is not used for advertising.**
   You own your data. Google Cloud does not process your data for advertising purposes.
4. **Know where Google stores your data and rely on it being available when you need it.**

   We publish the locations of our Google data centers; they are highly available, resilient, and secure.
5. **Depend on Google's independently-verified security practices.**

   Our adherence to recognized international security and privacy standards is certified and validated by independent auditors — wherever your data is located in Google Cloud.
6. **Trust that we never give any government entity "backdoor" access to your data or to our**

servers storing your data.

We reject government requests that are invalid, and we publish a transparency report for government requests.

See the data processing terms for Google Cloud Platform and G Suite for further details.

Data access

Customers own their data, not Google. At Google Cloud, we do not access customer data for any reason other than those necessary to fulfill our contractual obligations. Only a small group of Google employees, such as those who support authorized customer administrators, have access to customer data. Our employees' access rights and levels are based on their job function and role, using the concepts of least-privilege and need-to-know basis. To learn more, refer to Google's data access restrictions. Furthermore, given our commitment to transparency, we provide customers with the ability to view logs that capture when, how, and why our administrators access customer content.

Additionally, Google will retain, return, destroy, or delete personal data in accordance with the contract or service level agreements. To learn what happens when customer data is deleted in GCP and how long it takes to complete Google's data deletion process, refer to the Data deletion on Google Cloud Platform whitepaper.

Commitments to safeguarding individuals' privacy rights

GCP customers have administrative control over access to their data, allowing them to give individuals the right to access, amend, and obtain information (or copies of their personal information). To learn more, refer to details about our Cloud Identity & Access Management product, as described below.

GCP-managed security controls

Security is at the core of Google culture and our IT architecture, and we focus on innovating it every day. It is integral to our hiring process, employee training, and company-wide events to raise awareness and drive innovation in security. In addition, Google employs a dedicated security team comprising some of the world's foremost experts. This team maintains the company's defense systems, develops security review processes, builds security infrastructure, implements Google's security policies, and actively scans for security threats. To learn more, refer to the Cloud Data Processing Addendum.

Physical safeguards

Using defense-in-depth principles, Google has created a state-of-the-art IT infrastructure that provides a secure environment to support the deployment of services, storage of data with end-user privacy safeguards, communications between services, private communication with customers, and safe operation by administrators. We manage the security of this infrastructure in progressive layers starting with our data centers.

Google data centers feature layers of physical security protections. We limit access to these data centers to only a very small fraction of employees and have multiple physical security controls to protect our data center floors, such as biometric identification, metal detection, vehicle barriers, and custom-designed electronic access cards. We monitor our data centers 24/7/365 to detect and track intruders. Data centers are routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Data centers are typically connected via high-speed private links to provide secure and fast data transfer between them. This helps prevent data from being read, copied, altered, or removed without authorization during electronic transfer or transport, or while being recorded onto data storage media.

To learn more, refer to the Google Infrastructure Security Design Overview and our Data Centers page.

Technical safeguards

Google encrypts data at rest and encrypts data in transit, by default. The type of encryption used depends on the OSI layer, the type of service, and the physical infrastructure component. By default, we encrypt and authenticate all data in transit at one or more network layers when data moves outside physical boundaries not controlled by or on behalf of Google.

We offer several options for encryption key management. A fully managed encryption key service is provided by default that manages server-side encryption keys for customers; no setup or configuration is required. We also provide options for customers to supply their own keys and to fully manage their own encryption keys. Cloud Key Management System (KMS) is the service we provide for customers who choose to fully manage their own encryption keys.

To prevent unauthorized access by other tenants sharing the same physical infrastructure, we logically isolate our customers' data. We have a variety of isolation and sandboxing techniques for protecting a service from other services running on the same machine.

Additionally, we offer cutting-edge security tools to help customers manage their environments. For example, the Cloud Security Command Center for GCP brings actionable insights to security teams, and VPC Service Controls help to establish virtual security perimeters for sensitive data. To learn more, refer to our Security Products & Capabilities page.

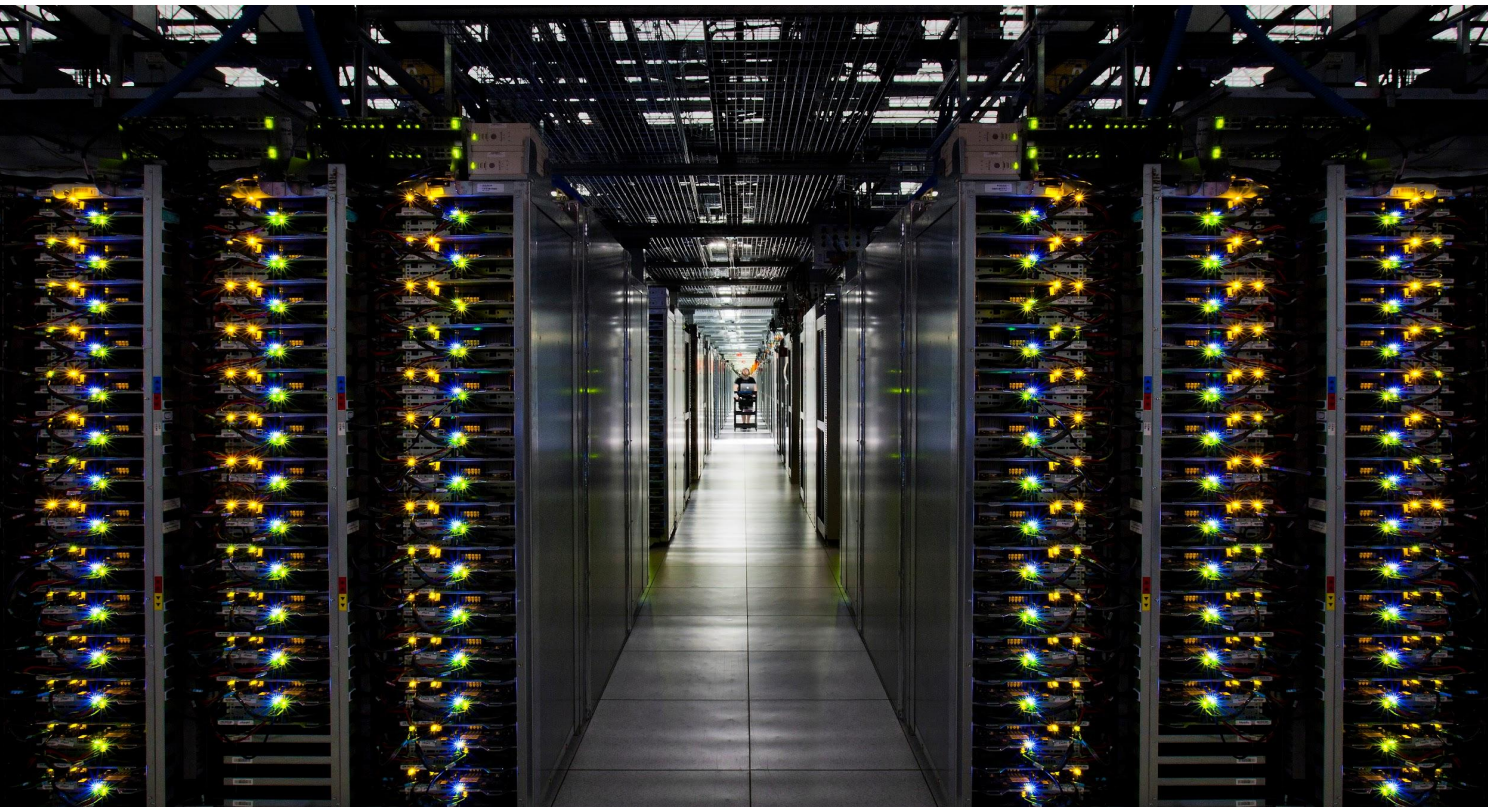
Administrative safeguards

Strong authentication and access controls restrict access to GCP production systems, internal support tools, and customer data. In particular, we design our systems to allow only authorized persons to access data; and ensure that personal data cannot be read, copied, altered, or removed without authorization during processing, use, and after recording. Google employs a centralized access management system to control personnel access to production servers, and provides access to only a limited number of authorized personnel. The granting or modification of access rights is based on concepts of least-privilege and need-to-know. Furthermore, Google ensures that all persons, including employees, contractors, and sub-processors, who are authorized to process customer data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. To learn more, consult our Cloud Data Processing Addendum (formerly Data Processing Terms).

Vulnerability management and threat monitoring

Google's vulnerability management process 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 tracks and follows up on vulnerabilities.

In addition, the security team periodically evaluates critical systems against a defined set of security health check guidelines. Our security monitoring program gathers information from internal network traffic, employee actions on systems, and outside knowledge of vulnerabilities to discover what might affect infrastructure integrity. Furthermore, management performs regular assessments of the control environment for specific areas, such as identity management, source code management, and authentication controls.



System reliability and availability

At GCP, we plan on our services being always available, even when we are upgrading our services or maintaining our systems. We designed our world-class infrastructure with system redundancy as a core element to keep services running 24/7/365. We have data centers geographically distributed to minimize the effects of disruptions caused by local and regional incidents. Google's highly redundant and dispersed infrastructure helps customers protect themselves from data loss, and enables them to build resilient and highly available systems by deploying resources across multiple regions and zones. Furthermore, the service level agreements for our offerings meet the business and operational requirements across various industries. To learn more about GCP's reliability and availability, read the Low Latency and Highly Available Solution section in the Google Security whitepaper.

GCP's incident management and breach notification process

Google has a rigorous process for managing data incidents. This process specifies actions, escalations, mitigation, resolution, and notification of potential incidents that can impact the confidentiality, integrity, or availability of our customer data. We promptly notify our customers if we detect a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to their data on systems that we manage. Moreover, we assist with investigative efforts via our support team.

In addition, our Cloud Data Processing Addendum and Business Associate Agreement contain provisions around data incident notification. For detailed information on, please reference the Google Incident Response Process.

Google has a rigorous data incident management process that specifies actions, escalations, mitigation, resolution, and notification of any potential incidents impacting the confidentiality, integrity, or availability of customer data.

GCP's compliance with standards and regulations

While the HHS does not recognize a formal certification process for HIPAA compliance, Google Cloud regularly undergoes several independent audits to assess the security, privacy, operational, and compliance controls we have in place based on global standards that encompass requirements outlined in HIPAA. HIPAA compliance is a shared responsibility between our customers and us, and we work continuously to ensure the highest level of controls.

What's more, we have dedicated internal teams that review compliance with security standards and regulations around the world. This team facilitates and supports independent audits and assessments by third parties in order to earn your trust.

Below are our certifications and assessments most relevant to the healthcare industry. To learn more, refer to our Standards, Regulations, and Certifications page.

ISO 27001

The International Organization for Standardization (ISO) 27001 is a security standard that outlines and provides the requirements for an information security management system. The 27001 standard lays out a framework and checklist of controls that allow Google to ensure a comprehensive and continually improving model for security management. GCP is certified as ISO 27001 compliant.

ISO 27017

The ISO/IEC 27017:2015 gives guidelines for information security controls applicable to cloud services by providing additional implementation guidance for relevant controls specified in ISO/IEC 27002. GCP is certified as ISO 27017 compliant.

ISO 27018

The ISO 27018 is a "Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors." This standard focuses primarily on security controls for public cloud service providers acting as PII processors. GCP is certified as ISO 27018 compliant.

SOC 2 and SOC 3 (SSAE 16/ISAE 3402 Type II)

Service Organization Controls (SOC) reports — SOC 2 and SOC 3 — evaluate an organization's information systems and controls with respect to security, availability, processing integrity, and confidentiality or privacy based on the existing SysTrust and WebTrust principles. The Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA) created the Statement on Standards for Attestation Engagements No. 16 (SSAE 16), which aligns closely with the International Standard on Assurance Engagements 3402

(ISAE 3402). SSAE 16 and ISAE 3402 are used to generate a report by an objective third party attesting to a set of statements that an organization asserts about its controls. Google Cloud undergoes a regular third-party audit to certify individual products against the SOC 2 and SOC 3 standards.

HITRUST CSF

HITRUST CSF is a security framework based on nationally and internationally accepted standards, including ISO, NIST, PCI, and HIPAA. Developed by the not-for-profit HITRUST, this framework contains a set of prescriptive security controls that relate to the organizational processes and technical controls for processing, storing, and transmitting sensitive data. GCP is certified under HITRUST CSF.

CSA STAR

The Cloud Security Alliance's Security, Trust & Assurance Registry Program (STAR) is a three-tiered provider assurance program of self-assessment, third-party audit, and continuous monitoring that aids customers with due diligence of cloud service providers in regard to security. GCP has completed the CSA STAR Level 1: Self-Assessment.

PCI DSS

Established by the major credit card associations, the PCI Security Standards Council is a global forum for the ongoing development, enhancement, storage, dissemination, and implementation of security standards for account data protection. To better protect cardholder data, the PCI Security Standards Council created the Payment Card Industry (PCI) Data Security Standards (DSS) as a set of network security and business best practice guidelines that establish a "minimum security standard" to protect customers' payment card information. Google Cloud undergoes an annual third-party audit to certify individual products against the PCI DSS. This means that these services provide an infrastructure upon which customers may build their own services or applications that store, process, or transmit cardholder data. For a list of GCP services that are PCI DSS 3.2 compliant, refer to our PCI DSS compliance page.

The Shared Responsibility Model

Under the Shared Responsibility Model, the cloud customer and its cloud service provider share the responsibilities of managing the IT environment, including those related to security and compliance. Shared responsibility enables our customers to allocate resources more effectively by reducing the amount of effort needed to provision and support their IT environment. The Shared Responsibility Model does not remove the accountability and risk from customers using our services, but it does help relieve the burden as we manage and control system components and physical control of facilities. It also shifts a portion of the cost of security and compliance onto Google Cloud from customers. Note

that customers are ultimately responsible for ensuring their own HIPAA compliance. One of the key responsibilities for a customer is to determine whether they are a “covered entity” (or a “business associate” thereof) and, if so, whether they require a BAA with Google for the purposes of the engagement. While Google Cloud provides secure and compliant offerings, the customer must ensure that the environment and applications that it builds on top of GCP are properly configured and secured according to HIPAA requirements.

Using GCP's solutions to support HIPAA compliance

This section identifies GCP products and services covered by the BAA and describes how customers can implement those offerings to support their HIPAA compliance.

Topics covered in this section

Disclaimer

The list of BAA-covered products and services is current as of March 2023. Please visit our Compliance page or contact your Google Cloud account representative to check for updated information.

GCP's Business Associate Agreement (BAA)

Customers who are subject to HIPAA and want to use GCP for their business purposes involving PHI must enter into a BAA with Google that covers specific Google Cloud products and services. To help customers use our offerings in line with HIPAA, we recommend that they follow these best practices.

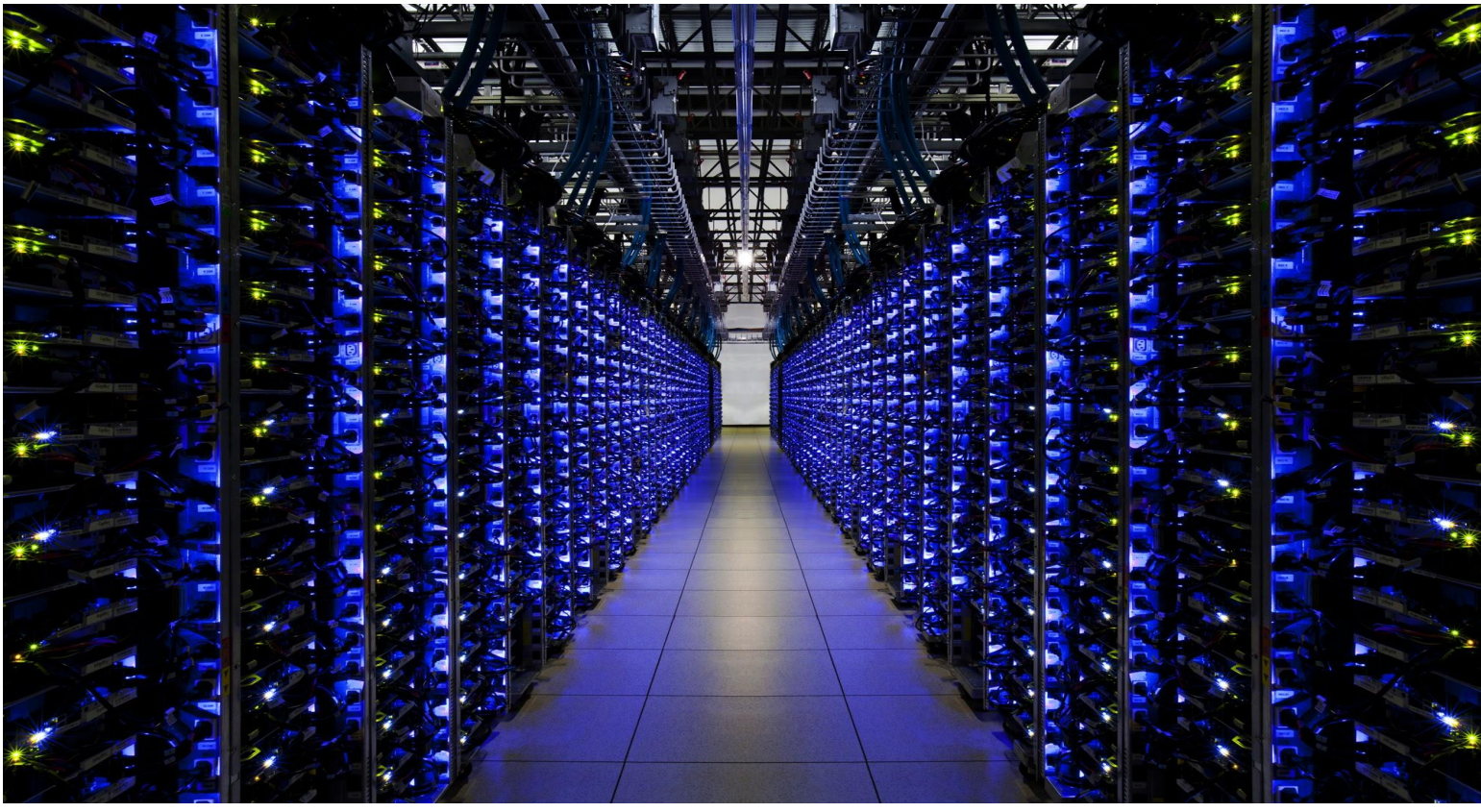
The GCP BAA covers GCP's entire infrastructure (all regions, all zones, all network paths, all points of presence) and the GCP services identified here.

Generally available privacy and security features across our offerings

There are numerous privacy and security features that apply across GCP that customers can leverage to help them satisfy their obligations under HIPAA. In this subsection, we list several important technical, administrative, and physical safeguards that apply across our BAA-covered service offerings. Customers have the ability to manage these features.

Type	Privacy & Security Features
Technical safeguards	• Encryption for data in transit and encryption for data at rest, both by default, provide customers the capability to protect the privacy of ePHI. Refer to the GCP's Security Environment for more information. • Virtual Private Cloud (VPC) network provides configurable connectivity for the products that handle sensitive data, such as PHI. Customers can use VPC to control access to their applications and how their workloads connect regionally and globally. In the HIPAA context, customers may find the following specific features useful: (1) private access to some Google services through internal IPs, so they can avoid giving their service a public IP address; (2) configuration of an application's front end to receive Internet requests and shield its backend services from public endpoints; (3) disaster recovery through application retention, as well as backup GCP compute capacity during an incident; and (4) VPC flow logs to help with network monitoring, forensics, and real-time security analysis.
Administrative safeguards	• Cloud Identity and Access Management (Cloud IAM) enables administrators to authorize who can take action on specific resources, giving organizations control and visibility to centrally manage the cloud resources handling ePHI. For established organizations with complex organizational structures, hundreds of workgroups, and potentially many more projects, Cloud IAM provides a unified view into access control across the entire organization, with built-in auditing to ease compliance processes. Users' access can be limited to only what they need to get the job done, and admins can easily grant default permissions to entire groups of users. • Google Cloud Audit Logging offers healthcare organizations a way to track activity in applications built on top of GCP and integrate logs with monitoring and log analysis tools. In particular, our Cloud Audit Logging maintains three audit logs for each project,
Administrative	

safeguards (continued)	folder, and organization: Admin Activity, System Events, and Data Access. Admin activity logs contain log entries for API calls or other administrative actions that modify the configuration or metadata of resources. Data access logs record API calls that create, modify, or read user-provided data. Data access audit logs are disabled by default because they can grow to be quite large; these logs can be enabled as desired. System Event logs contain log entries for when Compute Engine performs a system event. To learn more, refer to our Best practices for working with Google Cloud Audit Logging. • Cloud Logging allows healthcare organizations to store, search, analyze, monitor, and alert on log data and events in real time from any source, including GCP, other cloud services, and on-premises solutions. The information derived from Cloud Logging can be critical in determining whether a breach of ePHI has occurred and the extent to which it did.
Physical safeguards	• GCP is built with Google's trusted infrastructure that is designed to provide security through the entire data processing lifecycle, including ePHI. Google designed the infrastructure security in progressive layers, starting from our state-of-the-art physical security of data centers, continuing on to the security of the hardware and software that underlies the infrastructure, and finally, the technical constraints and processes in place to support operational security.



Cloud computing products and services

Customers can build and scale faster in a safe and secure manner using GCP's products and services in a HIPAA-aligned manner. Here we describe our computing offerings' unique privacy and security features that can support customers in their compliance with HIPAA. Note that this section is intended to highlight some features that customers may find useful in this context; it is not intended to be comprehensive, and it is subject to change.

Category	Products & Services	Privacy & Security Features
Compute	Google Compute Engine (GCE) GCE provides highly customizable virtual machines with best-of-breed features, pay-for-what-you-use pricing, and the option to deploy code directly or via containers.	• Provides secure connection to virtual machine instances with or without external IP addresses. • Provides ability to verify the identity of a virtual machine using instance identity tokens signed by Google, before an application built on GCE sends sensitive information to a virtual machine instance. • Provides more granular control over which users can connect to instances and what level of permission they have using Compute Engine IAM to manage SSH access to Linux instances. Customers could also manage instance access manually by adding and removing SSH keys in metadata.
	Google App Engine (GAE) GAE is a flexible platform-as-a-service for building scalable web applications and mobile and Internet of Things (IoT) backends; it lets healthcare organizations focus on their code, freeing them from many operational details of deployment and infrastructure management.	• Defines access rules with App Engine firewall and leverage managed SSL/TLS certificates by default on custom domains. These features, and others, help customers implement access management controls for their applications handling ePHI.
	Google Kubernetes Engine (GKE) GKE can be used by healthcare organizations to rapidly develop, deploy, update, and manage containerized applications. It lets customers use fully managed Kubernetes clusters to deploy, manage,	• Protects workloads on GKE at many layers of the stack, using authentication/authorization, node management, workload management, and others. • Provides configurable access control for GKE resources via Kubernetes role-based access control. • Allows users to authenticate and secure master-to-node, node-to-node, and instance-to-instance communications containing ePHI via trust built into GKE clusters.

Compute (continued)	and orchestrate Docker containers at scale that are configured with appropriate privacy and security controls.	• Safeguards passwords, OAuth tokens, SSH keys, and other sensitive information used by customers' GKE containerized applications in secure objects, with Secrets. Using Secrets reduces the risk of exposing this sensitive data to unauthorized users, helping increase the privacy of ePHI. • Monitors for unwanted API calls and investigates suspicious API requests in GKE containerized applications that are handling ePHI. Kubernetes Auditing provides a security-relevant chronological set of records documenting the sequence of activities that have affected the system by individual users, administrators, or other components of the system. • Provides configurable cluster networking, such as creating a private cluster that makes the master inaccessible from the public Internet. This feature enhances the security and privacy of ePHI being handled in GKE containerized applications. IP masquerading in clusters further increases security by preventing individual Pod IP addresses from being exposed to traffic outside link-local range and additional arbitrary IP ranges. • Provides configurable cluster security via PodSecurityPolicy and protects potentially sensitive cluster metadata with GKE resources.
	Google Cloud Functions A lightweight compute solution for developers to create single-purpose, stand-alone functions that respond to Cloud events without the need to manage a server or runtime environment.	• Can be invoked over HTTP(S). Each function is given a dedicated domain and a dynamically generated SSL/TLS certificate for secure communication. Result is returned in response to HTTP request.
Category	Products & Services	Privacy & Security Features
Storage	Google Cloud Storage (GCS) GCS allows for storage and retrieval of ePHI; it can be used for a range of scenarios, including production data storage, storing data for archival and disaster recovery. GCS has 99.999999999% annual durability and has high availability across all storage options.	• Several encryption options are available for protecting ePHI, including Google-managed encryption (by default), Customer-Managed keys, and Customer-Supplied keys. • Access Control Lists, in addition to IAM policies, can define who has access to buckets and objects, as well as what level of access, for purposes of sharing and collaborating while maintaining confidentiality. • Hashes and ETags helps detect whether data corruption has occurred.

Storage (continued)		• Signed URLs give time-limited read or write access to anyone in possession of the URL, regardless of whether the person has a Google account. • Signed Policy Documents allow visitors to upload files to GCS. • Firebase Security Rules can be used to authorize users and validate requests. Firebase SDKs add Google security to file uploads and downloads, from health-related images, audio, video, or other user-generated content. • Object Versioning can be used to protect data from being overwritten or accidentally deleted.
Category	Products & Services	Privacy & Security Features
Databases	Google Cloud SQL for MySQL A fully managed service that makes it easy for healthcare organizations to set up, maintain, manage, and administer MySQL relational databases to house critical healthcare data.	• MySQL user accounts provide security by controlling access to MySQL databases. • Cloud SQL Proxy provides secure access to Cloud SQL second-generation instances without having to whitelist IP addresses or configure SSL. • The High Availability configuration provides data redundancy, reducing downtime and ensuring that data continues to be available. • Backups provide a way to restore a Cloud SQL instance to recover lost data or recover from a problem with an instance. • Provides ability to install your own MySQL on GCE to keep the MySQL server and client applications on a private network.
	Google Cloud SQL for PostgreSQL A fully managed service that makes it easy to set up, maintain, manage, and administer a PostgreSQL relational databases to handle ePHI.	• PostgreSQL roles give control over what kind of access and capabilities users have when they access a PostgreSQL instance. • The High Availability configuration provides data redundancy, reducing downtime and ensuring that data continues to be available. • Backups provide a way to restore a Cloud SQL instance to recover lost data or recover from a problem with an instance.
	Google Cloud Bigtable Google Cloud Bigtable is a fully managed NoSQL database service suitable for handling petabytes of healthcare data, with access control, encryption, and audit logging features.	• Replication helps increase the availability and durability of data by copying it and automatically synchronizing copies across multiple zones. • Provide options to choose deployment location for resources to achieve business needs around latency, availability, and disaster recovery.

Databases (continued)	Google Cloud Spanner An enterprise-grade, globally distributed, and strongly consistent database service built for the cloud specifically to combine the benefits of relational database structure with non-relational horizontal scale; it revolutionizes database administration and management, and makes app development more efficient.	• Multilayer encryption protects customer data. • IAM integration for access and controls via Cloud Identity and Access Management (IAM) to control user and group access to Cloud Spanner resources at the project, Cloud Spanner instance, and Cloud Spanner database levels. • Audit logs for Admin Activity that is provided by default, and optional audit logs for Data Access, which record API calls that create, modify, or read user-provided data. • Replication of data benefits data availability.
	Google Cloud Datastore A highly scalable NoSQL database that is ideal for web and mobile applications that rely on highly available structured data.	• Provides high availability and consistency through a fully managed NoSQL database. • Ensures data integrity by executing multiple datastore operations in a single transaction with ACID (atomicity, consistency, isolation, durability) characteristics, so the grouped operations all succeed or all fail. • Supports multitenancy by creating separate data partitions for multiple client organizations, known as tenants. This allows customization of data values for each tenant, while keeping the same data schema for all tenants. It also makes provisioning of new tenants more efficient.
	Cloud Firestore A NoSQL document database built for automatic scaling, high performance, and ease of application development.	• Automatically encrypts data before it is written to disk. • Has built-in security access controls for data and enables simple data validation via a configuration language. • Provides ability to use custom security rules to implement role-based access control in your app.

Category	Products & Services	Privacy & Security Features
Networking	Google Cloud Load Balancing Scales applications on Google Compute Engine from zero to full-throttle. Distributes load-balanced compute resources in single or multiple regions, close to your users to meet high availability requirements. Cloud Load Balancing comes in a variety of flavors and is integrated with Google Cloud CDN for optimal	• Uses HTTP(S) load balancing to balance HTTP and HTTPS traffic across multiple backend instances, across multiple regions making the entire app available via a single global IP address, thereby resulting in a simplified DNS setup. For HTTPS traffic, it provides SSL termination and load balancing. • With TCP load balancing, the TCP traffic can be spread over a pool of instances within a Compute Engine region. • SSL proxy provides SSL termination for non-HTTPS traffic with load balancing. • SSL offload enables centrally managing SSL certificates and decryption.

Networking (continued)	application and content delivery.	• Includes advanced support features, such as IPv6 Global Load Balancing, WebSockets, user-defined request headers, and protocol forwarding for private VIPs.
Category	Products & Services	Privacy & Security Features
Migration	Google Transfer Appliance Service A custom-built hardware appliance and service for moving large amounts of data to Google Cloud quickly and securely.	• Tamper-evident seals are used on shipping cases, to and from customer data ingest site. • Data is encrypted with an industry standard AES 256 algorithm at the moment of capture and customers decrypt their own data once it is ingested into its final storage bucket. Once the transfer is complete, all of the data on the Transfer Appliance is erased per the NIST-800-88 standard. • Transfer Appliance Capture Utility calculates a hash of each source file when it is captured and preserves this hash for integrity checking during the data rehydration process. During rehydration, the Transfer Appliance Rehydrator calculates and compares the hashes of the files being rehydrated with the hashes computed when the files were captured. Verifying rehydrated data helps ensure data integrity. • Provides the ability to monitor storage disk status during a data capture to ensure data transfer completion and integrity. • Allows the user to keep track of the Transfer Appliance's geographic location while it is being transported.
Management tools	Cloud Logging A fully managed solution for storing, searching, analyzing, monitoring, and alerting on log data and events from any source including GCP and Amazon Web Services (AWS).	• Provides ability to read and write log entries, search and filter logs, export logs, and create logs-based metrics in order to, among other things, resolve issues in systems and applications. • Cloud Logs Viewer, APIs, and the gCloud CLI can be used to access audit logs that capture all the admin and data access events within GCP. • Allows the export of log data to GCS to archive for future use, such as auditing or postmortem analysis. • Fully integrates with Cloud Monitoring, Trace, Error Reporting, and Debugger; also integrates with Splunk and other third-party applications.
	Error Reporting A centralized error management interface to help identify and understand	• With IAM, every API method in Error Reporting requires that the account making the API request has the appropriate permissions to use the resource.

Management tools (continued)	crashes in applications that may be handling ePHI.	Permissions are granted by setting policies that grant roles to a user, group, or service account. • In addition to the primitive roles, which are Owner, Editor, and Viewer, it allows granting Error Reporting roles to the users of a project. • Writes System Event audit logs, containing log entries for when GCE performs a system event. It also writes audit logs for Admin Activity, which includes operations that modify the configuration or metadata of a resource. Both features are provided by default.
	Cloud Trace A distributed tracing system that can be used to understand the latency of an application handling health information in near real time.	• Uses GCP IAM to configure permissions and roles for users, groups, and service accounts that are supported by Stackdriver Trace. Also allows creation of custom roles with Stackdriver Trace permissions. • Writes System Event audit logs containing log entries for when GCE performs a system event. • If explicitly requested, it can write audit logs for Data Access, which record API calls that create, modify, or read user-provided data.
	Cloud Operations A dynamic code analysis product that help developers analyse poorly performing code and determine paths that consume the most resources and thereby increase the latency and cost of applications and web services.	• Controls access to profiling activities in Google Cloud Platform projects by using GCP IAM roles and permissions. • Writes System Event audit logs, containing log entries for when Compute Engine performs a system event. Profiler provides these logs by default. • Data Access audit logs record API calls that create, modify, or read user-provided data.
	Google Cloud Deployment Manager An infrastructure management service that makes it simple to automate the creation and deployment of GCP resources.	• Provides the ability to create and manage cloud resources that are configured with the proper privacy and security settings with simple templates and config files. • Provides the ability to add users as a project team member and grant them the appropriate IAM roles. IAM supports both predefined and primitive roles for Deployment Manager.
	Cloud Console A web admin user interface to manage and get insights into web applications, data analysis, virtual machines, datastore, databases, networking, and developer services relating to ePHI.	• Connects to your virtual machine instances via SSH directly from the browser. • Offers a single place to understand activities happening in cloud applications. Also enables tracking down issues and audit access. • Allows to manage and audit co-workers' access to project resources.

Category	Products & Services	Privacy & Security Features
Developer tools	Google Container Registry A centralized place to store, manage, and secure Docker images. Container Registry can be used to more rapidly deploy applications handling ePHI.	• Provides quick access to secure private Docker image storage and allows to maintain control over who can access, view, or download images. • In-depth scanning feature detects vulnerabilities in early stages of the software deployment cycle and helps ensure that container images are safe to deploy. In addition, constantly refreshed vulnerability database helps ensure that scans find the latest malware and other advanced threats.
	Google Cloud Source Repositories A single place hosted on GCP for a team to store, manage, and track code. Cloud Source Repositories can also be used to more rapidly develop applications that meet the privacy and security rules for ePHI.	• Enables security key detection to block git push transactions that contain sensitive information, in order to improve the security of source code. • Provides automatic logging via Stackdriver Logging to help data access tracking and troubleshooting. • Is integrated with GitHub and Bitbucket.

Analytics and machine learning products and services

Healthcare organizations can use Google Cloud's powerful analytics and machine learning tools to take full advantage of big data. Here we describe our products' and services' unique privacy and security features that can help customers meet their HIPAA obligations. Note that the features listed are not comprehensive.

Category	Products & Services	Privacy & Security Features
Data analytics	Google Cloud Pub/Sub A fully managed real-time messaging service that allows sending and receiving messages between independent applications. It brings the flexibility and reliability of enterprise message-oriented middleware to the cloud. Part of Google Cloud's stream analytics solution, Cloud Pub/Sub ingests event streams from sources such as medical devices and delivers them to Cloud Dataflow for processing and BigQuery for analysis.	• Provides many-to-many, asynchronous messaging that decouples senders and receivers, thereby allowing secure and highly available communication among independently written applications. • Employs fine-grained access controls to govern data sharing. • Provides end-to-end encryption for data pipelines.

Data analytics (continued)	Google Cloud Dataflow A fully managed service for transforming and enriching data in stream and batch modes.	• Provides a permissions system to maintain secure access to enterprise's pipeline files and resources, regardless of whether running locally or in the cloud. • Provides access to GCP resources across multiple GCP projects via Apache Beam pipelines. • Deploys special security mechanisms to keep data secure and private.
	Google BigQuery A fast, highly scalable, cost-effective, and fully managed cloud-based data warehouse for analytics, with built-in machine learning. BigQuery can be used to safely and quickly analyze massive amounts of health information.	• Allows to easily and securely share insights within an organization and beyond as datasets, queries, spreadsheets, and reports. • Provides automatic data replication for disaster recovery and high availability of processing for no additional charge. • Provides strong security with fine-grained identity and access-management control. • Uses encryption by default and Customer Managed Encryption Keys. • Provides rich monitoring, logging, and alerting through Cloud Audit Logs.
	Google Cloud Dataproc A fully managed service for running Apache Spark and Apache Hadoop clusters. This is particularly useful for organizations extracting, transforming, and loading huge amounts of medical data from a variety of sources for subsequent analysis.	• In addition to default encryption, provides Customer Managed Encryption Keys as an option to encrypt data on the Persistent Disks associated with the VMs in a Cloud Dataproc cluster and/or the cluster metadata and job driver output written to the Cloud Storage bucket used by Cloud Dataproc. • Utilizes Cloud Dataproc Granular IAM to grant permissions at the cluster, jobs, operations, or workflow template level. • Seamlessly integrates with other BAA-covered services such as BigQuery, GCS, Bigtable, Cloud Logging, and Cloud Debugger.
	Looker An enterprise platform for business intelligence, data applications, and embedded analytics that helps customers explore and share insights in real time.	• Runs on Google Compute Engine (GCE) that has completed ISO 27001, SSAE 16, SOC 1, SOC 2, and SOC 3 certifications. • GCE's ability to connect to multiple cloud services allows it to focus on data science tasks. Its innovative data centers and Live Migration technology enable proactive infrastructure maintenance, improving reliability and security. • Provides built-in access control.

	Cloud Life Sciences A technology designed to securely and efficiently process petabytes of genomic data so that the life science community can organize the world's genomic information and make it accessible and useful.	• Leverages Google Cloud Storage for storing genomic data. • Uses secure protocols to access and share genomic data using Google's implementation of the htsget protocol defined by the Global Alliance for Genomics and Health.
Category	**Products & Services**	**Privacy & Security Features**
Artificial intelligence (AI) and machine learning (ML)	Vertex AI A managed service that enables developers and data scientists to build superior ML models with training and prediction, and deploy them into production. Machine Learning Engine can be used to analyze ePHI and deliver insights to physicians that will improve diagnosis and better inform patient care.	• Provides ability to control access to resources and safely/securely share models, and to generate Admin Activity and Data Access logs for API operations.
	Google Cloud Natural Language API Natural language understanding technology to derive insights from unstructured text through powerful pretrained machine learning models in an easy-to-use REST API and through custom models that are easy to build with AutoML Natural Language.	• For API-based services, customers benefit from GCP's native security and privacy capabilities. These services have minimal customer responsibilities under our Shared Responsibility Model. Users should ensure appropriate access control and usage of these services per their specific requirements.
AI and ML (continued)	Google Cloud Speech API Speech-to-text conversion technology powered by machine learning.	• For API-based services, customers benefit from GCP's native security and privacy capabilities. These services have minimal customer responsibilities under our Shared Responsibility Model. Users should ensure appropriate access control and usage of these services per their specific requirements.
	Google Cloud Translation API Cloud-based technology to dynamically translate between languages by using pretrained models and/or building custom models specific to enterprise needs, using AutoML Translation. Cloud Translation API's HIPAA-related use cases include translation support	• For API-based services, customers benefit from GCP's native security and privacy capabilities. These services have minimal customer responsibilities under our Shared Responsibility Model. Users should ensure appropriate access control and usage of these services per their specific requirements.

for healthcare provider communications with a diverse set of patients.	
Google Cloud Vision API Derive insight from images with Google's powerful pretrained API models or easily train custom vision models with AutoML Vision, such as for analyzing medical images to diagnose diseases.	• For API-based services, customers benefit from GCP's native security and privacy capabilities. These services have minimal customer responsibilities under our Shared Responsibility Model. Users should ensure appropriate access control and usage of these services per their specific requirements.
Google Cloud Video Intelligence API Video analysis technology that extracts metadata with an easy-to-use REST API. HIPAA-related application of Cloud Video Intelligence API includes facial and body movement analysis to incorporate non-verbal cues into mental health diagnosis.	• For API-based services, customers benefit from GCP's native security and privacy capabilities. These services have minimal customer responsibilities under our Shared Responsibility Model. Users should ensure appropriate access control and usage of these services per their specific requirements.
Cloud Healthcare API The Cloud Healthcare API bridges the gap between care systems and applications built on Google Cloud.	• Provides standards-based APIs powering actionable healthcare insights for security and compliance-focused environments in healthcare technologies. • Connects data to advanced Google Cloud capabilities, including data processing with Cloud Dataproc, scalable analytics with BigQuery, and machine learning with Cloud ML Engine, while also simplifying application development and device integration.

Identity and security products and services

Google Cloud's security solutions enable healthcare organizations to protect individuals' identities and help them meet their policy, regulatory, and business objectives. Here we describe our products' and services' unique privacy and security features that can help customers on their compliance journey. Note that the features below are not comprehensive.

Category	Products & Services	Privacy & Security Features
Identity	Cloud Identity Manage user identities and devices in one highly secure Identity-as-a-Service (IDaaS) platform.	• Provides user lifecycle management of identities as people join, move, change roles, and leave the organization. Provides ability to create or import user accounts into a cloud-based directory to easily provision or deprovision accounts.

		• Provides ability to manage Android, iOS, Chrome browser, and other desktop devices from a central console. Provides the ability to enforce enterprise security policies for personal devices, implement screen locks or passcodes, wipe corporate data, view and search for devices, and export details. • Protects user accounts with multifactor authentication (i.e., two-step verification) methods like push notifications and one-time passwords (OTPs) to protect organization-owned resources. Enforces the use of phishing-resistant security keys for high-value users and applications. • Increases user convenience and security by allowing users to access multiple apps using the same credentials, i.e., Single Sign-on. Hundreds of pre-integrated SAML 2.0 and OpenID Connect apps are supported, in addition to custom apps that use Google as an identity provider. • Provides ability to build a catalog of pre-approved third-party SaaS apps and enterprise mobile applications that users can access. Ensures visibility and compliance. • Allows user to monitor security and compliance posture with reporting and auditing capabilities, including logins and third-party app use. Alerts are received for suspicious activity. • Provides ability to integrate cloud and on-premise directories so that all identities are managed in one place. • Integrates with hundreds of cloud applications using one IDaaS.
Category	**Products & Services**	**Privacy & Security Features**
Security	Google Cloud Identity-Aware Proxy (Cloud IAP) Use identity and context to guard access for applications deployed on GCP.	• Verifies user identity and context of an access request to determine if a user should be allowed to access the cloud application. • Establishes a central authorization layer for applications accessed by HTTPS, in order to use an application-level access control model instead of relying on network-level firewalls. Defines access policies centrally and applies them to all of your applications and resources. • Creates granular access control policies to GCP-hosted applications based on attributes like user identity, device security status, and IP address.

		• Configures a single layer of security to manage user access to cloud applications and improve security with security key enforcement to prevent phishing.
	Google Cloud Data Loss Prevention (DLP) Cloud DLP is a security service that can automatically discover and redact sensitive data.	• Allows users to better understand, manage, and redact sensitive data. Also provides the ability to optionally redact data using techniques like masking, secure hashing, generalization and bucketing, date shifting, and format-preserving encryption. • Provides the ability to classify or automatically redact sensitive data from text streams, and within images, before writing to disk, generating logs, or performing analysis. Also used to detect and classify sensitive data within storage and databases. Users can integrate Cloud DLP into their applications so that they screen data for sensitive content before storing it. • Provides the ability to classify, mask, tokenize, and transform sensitive elements in real time to help better manage the data collected, stored, or used for business or analytics. For example, create a custom regex detector for medical record numbers to detect matches based on a regex pattern. And, features like format-preserving encryption help preserve the utility of data for joining or analytics while obfuscating the raw sensitive identifiers. • Uses risk analysis methods before de-identification to help determine an effective de-identification strategy, or after de-identification to monitor for any changes or outliers.
Security (continued)	Google Cloud Resource Manager Hierarchically manage resources by project, folder, and organization to safeguard ePHI.	• The Organization Policy Service provides centralized and programmatic control over an organization's cloud resources and lets the administrator configure restrictions across the entire resource hierarchy. • Protects projects from accidental deletion with liens.
	Google Cloud Key Management Service (Cloud KMS) Cloud-hosted key management service.	• Creates, uses, rotates, automatically rotates, and destroys industry-strength symmetric and asymmetric cryptographic keys. • Uses a key to encrypt, decrypt, or sign data such as secrets for storage. • Encrypts data with a symmetric or asymmetric key that is under enterprise control. Performs signing

		operations with RSA and elliptic curve keys of various lengths. • Ensures appropriate secret management; that is, secure secrets — small pieces of sensitive data at build or run time. • Implements a key hierarchy with a local data encryption key (DEK), protected by a key encryption key (KEK) in Cloud KMS. Manages keys used to encrypt data at the application layer, stored in storage systems, at Google, or anywhere else. Uses additional authenticated data as an integrity check and to help protect data from a confused deputy attack. • Rotates an asymmetric key at will, and also sets a rotation schedule for symmetric keys to automatically generate a new key version at a fixed time interval. Multiple versions of a symmetric key can be active at any time for decryption, with only one primary key version used for encrypting new data. • Manages the encryption keys used to protect sensitive data residing across GCP with Customer Managed Encryption Keys. For compliance mandates requiring that keys and crypto operations be performed within a hardware environment, the Cloud KMS integration with Cloud HSM makes it simple to create a key protected by a FIPS 140-2 Level 3 device. • The built-in 24-hour delay for key material destruction prevents accidental or malicious data loss.
Security (continued)	Google Cloud VPN An IPsec VPN tunnel used to securely extend an on-premises network to Google's network when transmitting ePHI.	• Securely connects an on-premises network to the GCP Virtual Private Cloud network through an IPsec VPN connection. • Traffic traveling between the two networks is encrypted by one VPN gateway, then decrypted by the other VPN gateway.
	Cloud Armor Protects your services against denial of service and web attacks using Google's global infrastructure and security systems.	• Works with the HTTP(S) Load Balancer to provide built-in infrastructure DDoS defense. • Creates rules using any combination of L3–L7 parameters and geolocation to protect your deployment with a flexible rules language. Also uses predefined rules to defend against cross-site scripting (XSS) and SQL injection defense. • Configures security policies with a hierarchy of rules. Applies a policy to one or more services.

- Enforces access control based on IPv4 and IPv6 addresses.
- Identifies and enforces access control based on geographic location of incoming traffic.
- Enables Preview mode to understand service access patterns before enabling your policies and to ensure the correct traffic sources are being allowed and blocked.

Additional Google Cloud security-related resources

Our customers are responsible for ensuring they are HIPAA compliant and Google Cloud our customers by providing services on a highly secure, controlled platforma wide array of security products and services. Our platform, tools, and resources can help customers meet regulatory requirements and reduce the technical burden and cost of compliance.

The additional products and features listed below may be helpful in developing and managing applications. Customers should use these appropriately for their applicable use cases and in the context of the BAA.

Category	Products & Services	Description
Governance	Asset Tracking	Accurate, real-time global location data for fleets, assets, and devices.
	Cloud Console Mobile App	Manage GCP services from your Android or iOS device.
	Cloud Endpoints	Develop, deploy, and manage APIs on any Google Cloud backend.
	Cloud Shell	Manage infrastructure and applications from the command line in any browser.
Governance (continued)	Cloud Operations	Monitoring and management for services, containers, applications, and infrastructure.
	Cloud Monitoring	Provides visibility into the performance, uptime, and overall health of applications running on GCP and AWS.
Identity & Access Management	Firebase Authentication	Simple, free multi-platform sign-in.
	Security Keys	Prevent phishing with security keys.
Data Security	Cloud Hardware Security Module (HSM)	Protect your cryptographic keys in a fully managed, cloud-hosted HSM service.
Network Security	Application Layer Transport Security	Mutual authentication and transport encryption system.

	VPC Service Controls	Define secure access zones for sensitive data in GCP services.
Infrastructure Security	Binary Authorization	Deploy only trusted containers on Kubernetes Engine.
	Container Security	Secure your container environment on GCP.
	Shielded VMs	Hardened GCE virtual machines.
Endpoint Security	Chromebooks	Easy to use, get faster over time, and are built from the ground up to be secure.
	Chrome Browser	Protection at every layer of the product, from malware and phishing protection to state-of-the-art sandboxing and network security.
	Chrome OS	Protect Chrome devices with enterprise-grade security.
	Safe Browsing API	Protect devices by showing warnings to users across Google products.
Application Security	Apigee	Design, secure, analyze, and scale APIs anywhere.
	Cloud Security Scanner	Automatically scan your App Engine apps.
Security Monitoring & Operations	Access Transparency	Expand visibility over your cloud provider through near-real-time logs.
	Cloud Security Command Center	A comprehensive security and data risk platform.

Conclusion

This guide describes how customers can securely store, analyze, and gain insights from health information with GCP offerings while meeting HIPAA compliance requirements. We provide this information to assist customers in determining which GCP products are suitable for them and in understanding how to design, build, and deploy applications on GCP that will handle sensitive health information safely and securely.

This guide is for informational purposes only. Google does not intend the information or recommendations in this guide to constitute legal advice. Each customer should independently evaluate its own particular use of the services, as appropriate, in order to support its legal and regulatory compliance obligations. Customers are ultimately responsible for ensuring that they use GCP in compliance with HIPAA.

Additional resources

To learn more about G Suite in relation to HIPAA, refer to the HIPAA Compliance with G Suite and Cloud Identity article and the G Suite and Cloud Identity HIPAA Implementation Guide.

Learn more		Engage	
Learn why other organizations are choosing Google Cloud	Why Google Cloud?	**Try Google Cloud for free**	GCP Free Tier
Learn more about our services	Google Cloud Solutions	**Call our Knowledge Center**	844-613-7589
Learn more about our pricing	Google Cloud Pricing		

Act		Get support	
Get Google on your team	Fill out this form or call 844-613-7589	**Frequently asked questions**	GCP FAQs
Train your team	Google Cloud Training	**Customer technical support**	Contact our Google Cloud Support Center
Quickstarts – *Deploy your first solution in 10 minutes or less*	Getting Started With GCP