HIPAA Compliance on Google Cloud Platform

Google Cloud

Table of Contents

Disclaimer

This guide is for informational purposes only. Google does not intend the information or recommendations in this guide to constitute legal advice. Each customer is responsible for independently evaluating its own particular use of the services as appropriate to support its legal compliance obligations.

Intended Audience

For customers who are subject to the requirements of the Health Insurance Portability and Accountability Act (known as HIPAA, as amended, including by the Health Information Technology for Economic and Clinical Health — HITECH — Act), Google Cloud Platform supports HIPAA compliance. This guide is intended for security officers, compliance officers, IT administrators, and other employees who are responsible for HIPAA implementation and compliance on Google Cloud Platform. After reading this guide, you will understand how Google is able to support HIPAA compliance as well as understand how to configure Google Cloud Projects to help meet your responsibilities under HIPAA.

Definitions

Any capitalized terms used but not otherwise defined in this document have the same meaning as in HIPAA. Furthermore, for the purposes of this document, Protected Health Information (PHI) means the PHI Google receives from a Covered Entity.

Overview

This guide covers HIPAA compliance on Google Cloud Platform. HIPAA compliance for G Suite is covered separately.

It is important to note that there is no certification recognized by the US HHS for HIPAA compliance and that complying with HIPAA is a shared responsibility between the customer and Google. Specifically, HIPAA demands compliance with the Security Rule, the Privacy Rule, and the Breach Notification Rule. Google Cloud Platform supports HIPAA compliance (within the scope of a Business Associate Agreement) but ultimately customers are responsible for evaluating their own HIPAA compliance.

Google will enter into Business Associate Agreements with customers as necessary under HIPAA. Google Cloud Platform was built under the guidance of a more than 700 person security engineering team, which is larger than most on-premise security teams. Specific details on our approach to security and data protection including details on organizational and technical controls regarding how Google protects your data, can be found in the Google Security Whitepaper and Google Infrastructure Security Design Overview.

In addition to documenting our approach to security and privacy design, Google undergoes several independent third party audits on a regular basis to provide customers with external verification (reports and certificates are linked below). This means that an independent auditor has examined the controls present in our data centers, infrastructure and operations. Google has annual audits for the following standards:

SSAE16 / ISAE 3402 Type II. Here is the associated public SOC 3 report. The SOC 2 report can be obtained under NDA.

ISO 27001. Google has earned ISO 27001 certifications for the systems, applications, people, technology, processes and data centers serving Google Cloud Platform. Our ISO 27001 certificate is available on the compliance section of our website.

ISO 27017, Cloud Security. This is an international standard of practice for information security controls based on the ISO/IEC 27002 specifically for cloud services. Our ISO 27017 certificate is available on the compliance section of our website.

ISO 27018, Cloud Privacy. This is an international standard of practice for protection of personally identifiable information (PII) in public cloud services. Our ISO 27018 certificate is available on the compliance section of our website.

FedRamp ATO for Google App Engine

PCI DSS v3.1

In addition to ensuring the confidentiality, integrity and availability of Google environment, Google's comprehensive third party audit approach is designed to provide assurances of Google's commitment to best in class information security. Customers may reference these third party audits reports to assess how Google's products can meet their HIPAA compliance needs.

Customer Responsibilities

One of the key responsibilities for a customer is to determine whether or not they are a Covered Entity (or a Business Associate of a Covered Entity) and, if so, whether they require a Business Associate Agreement with Google for the purposes of their interactions.

While Google provides a secure and compliant infrastructure (as described above) for the storage and processing of PHI, the customer is responsible for ensuring that the environment and applications that they build on top of Google Cloud Platform are properly configured and secured according to HIPAA requirements. This is often referred to as the shared security model in the cloud.

Essential best practices:

- ☐ Execute a Google Cloud BAA. You can request a BAA directly from your account manager.
- ☐ Disable or otherwise ensure that you do not use Google Cloud Products that are no explicitly covered by the BAA (see Covered Products) when working with PHI.

Recommended technical best practices:

- ☐ Use IAM best practices when configuring who has access to your project. In particular, because service accounts can be used to access resources, ensure access to those service accounts and service account keys is tightly controlled.
- ☐ Determine whether your organization has encryption requirements beyond what is required by the HIPAA security rule. All customer content is encrypted at rest on Google Cloud Platform, see our encryption whitepaper for further details and any exceptions.
- ☐ If you are using Cloud Storage, consider enabling Object Versioning to provide an archive for that data and to allow for undelete in the case of accidental data deletion. Furthermore, review and follow the guidance provided in Security and Privacy Considerations before using `gsutil` to interact with Cloud Storage.
- ☐ Configure audit log export destinations. We strongly encourage exporting audit logs to Google Cloud Storage for long term archival as well as to Google BigQuery for any analytical, monitoring, and/or forensic needs. Be sure to configure access control for those destinations appropriate to your organization.

- [ ] Configure access control for the logs appropriate to your organization. Admin activity audit logs can be accessed by users with the Logs Viewer role and data access audit logs can be accessed by users with the Private Logs Viewer role.

- [ ] Regularly review audit logs to ensure security and compliance with requirements. As noted above, BigQuery is an excellent platform for large scale log analysis. You may also consider leveraging SIEM platforms from our partners such as Splunk, Netskope, LogEntries and Tenable Network Security to demonstrate compliance through log analysis.

- [ ] When creating or updating resources, be sure to avoid including PHI or security credentials when specifying a resource's metadata as that information may be captured in the logs. Audit logs never include the data contents of a resource or the results of a query in the logs, but resource metadata may be captured.

Covered Products

The Google Cloud BAA covers GCP's entire infrastructure (all regions, all zones, all network paths, all points of presence), and the following products:


Google BigQuery


Google Cloud Bigtable


Google Cloud Dataflow


Google Cloud Dataproc


Google Cloud Storage


Google Cloud SQL


Google Compute Engine


Google Container Engine


Google Container Registry


Google Genomics

Please refer to the Cloud Platform compliance site for the most current list of covered products. This list is updated as new products become available to the HIPAA program.

Unique Features

GCP's security practices allow us to have a HIPAA BAA covering GCP's entire infrastructure, not a set aside portion of our cloud. As a result, you are not restricted to a specific region which has scalability, operational and architectural benefits. You can also benefit from multi-regional service redundancy as well as the ability to use Preemptible VMs to reduce costs.

The security and compliance measures that allow us to support HIPAA compliance are deeply ingrained in our infrastructure, security design, and products. As such, we can offer HIPAA regulated customers the same products at the **same pricing** that is available to all customers, including sustained use discounts. Other public clouds charge more money for their HIPAA cloud, we do not.

Conclusion

Google Cloud Platform is the cloud infrastructure where customers can securely store, analyze and gain insights from health information, without having to worry about the underlying infrastructure.

Appendix

Useful References

Google Security Whitepaper
Google Infrastructure Security Design Overview
HIPAA Government Website
HHS Guidance on HIPAA compliance and Cloud Computing

Google Cloud