May 20, 2021

To: Sundar Pichai, CEO

Halimah DeLaine Prado, General Counsel

From: Kathryn Van Sistine

University of St. Thomas

Re: Google: Ensuring Clients' HIPAA Compliance

Executive Summary

Google's system of allowing clients to interact with the Health Insurance Portability and Accountability Act (HIPAA)'s protected health information (PHI) using Google's services presents multiple compliance issues. These issues range from data security to Google's liability for a client's failure to comply with HIPAA's standards. However, Google thrives in this complicated regulatory environment through their effective compliance program. It starts with Google's security culture demonstrated in and implemented through their Code of Conduct. It's augmented through external audits to keep Google's systems up to global compliance certifications' standards, employee background checks, administrative safeguards, training throughout Googlers' careers, and the tone from the top's encouragement to go beyond the minimum required by law. Google ensures that all Google services are compliant with HIPAA regulations and that clients must use these baseline services to ensure that PHI is protected.

Google also defends itself against liability through the Shared Responsibility Model, the Business Associate Agreement (BAA) requirement, and the Google Cloud Healthcare Data Protection Toolkit. The Shared Responsibility Model clarifies to clients that Google and the client share the responsibility of protecting HIPAA data. Since all clients who want to interact with PHI are required to sign a BAA with Google, it ensures that both parties have stipulated to being in compliance with HIPAA standards and outlines each party's responsibilities. Google's healthcare toolkit reminds clients of their HIPAA obligations and provides them with resources encouraging them to go beyond compliance's baseline.

Google's compliance program follows the Seven Pillars and the two foundations to create competitive differences that will increase revenue and present mitigating factors if issues arise.

Background Information

HIPAA Overview

The Health Insurance Portability and Accountability Act (HIPAA) of 1996[1] is a federal law requiring the creation of national standards to protect patient health information from being disclosed without a patient's consent or knowledge. The U.S. Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule[2] to generate standards addressing the use and disclosure of patient's protected health information (PHI) by covered entities subject to the Privacy Rule. Covered entities include healthcare providers, health plans (entities that provide or pay medical care costs), healthcare clearinghouses (entities that receive identifiable health information only when providing processing services to a health plan or healthcare provider), and business associates (person or organization using or disclosing individually identifiable health information in order to assist a covered entity through services such as claims processing, data analysis, utilization review, and billing). The standards govern their transactions such as claims, benefit eligibility inquiries, and referral authorization requests. The HIPAA Privacy Rule's goal is to make sure that individuals' PHI is secure while still allowing access to the health information necessary to provide health care.

Permitted Uses and Disclosures of Protected Health Information

In the following circumstances outlined by the Centers for Disease Control and Prevention, covered entities are allowed to use and disclose protected health information[3]:

- Disclosure to the patient
- Treatment, payment, and healthcare operations for the patient
- Opportunity to agree or object to the disclosure of PHI
- Public interest and benefit activities

The HIPAA Security Rule

The HIPAA Security Rule[4] involves the protection of a subset of information covered by the HIPAA Privacy Rule and applies to all covered entities. It involves all individually identifiable health information created, received, maintained or transmitted in an electronic form by a covered entity. These transactions involve what is known as "electronic protected health information."

The following list from the Center for Disease Control and Prevention includes what all covered entities must do to be in compliance with the HIPAA Security Rule[5]:

- Ensure the confidentiality, integrity, and availability of all electronic protected health information
- Detect and safeguard against anticipated threats to the security of the information
- Protect against anticipated impermissible uses or disclosures

---

[1] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf

[2] https://www.law.cornell.edu/regulations/missouri/9-CSR-10-5-220

[3] https://www.cdc.gov/phlp/publications/topic/hipaa.html

[4] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf

[5] https://www.cdc.gov/phlp/publications/topic/hipaa.html

- Certify compliance by their workforce

The HIPAA Journal[6] evaluated Google's compliance with HIPAA standards and determined that Google Apps and G Suite do support HIPAA compliance through providing the necessary controls. Google does not violate HIPAA rules provided that HIPAA's rules are also followed by Google's clients and users. Google can be used by HIPAA's covered entities to share PHI, provided that the account is configured correctly and the standard security practices are applied. This requires the PHI vendor to sign a HIPAA-compliant Business Associate Agreement (BAA) stating that both organizations (Google and the vendor) comply with HIPAA's regulations. This requires that PHI can only be shared or used via Google services that are explicitly covered by the BAA. This excludes third party apps used in conjunction with G Suite products.

Recommendations for Implementation

Google's Code of Conduct

Google's first step in implementing a culture of compliance is having a clear Code of Conduct[7] that is integrated throughout the organization. Google's communication and integration of their Code of Conduct is demonstrative of COSO's model of internal controls. It creates a compliance-oriented culture from the top of the organization and demonstrates its applicability through all levels of the organization. Google makes it clear that all employees, Board members, and their extended workforce (temporary workers, vendors, and independent contractors) must follow the code. The company clearly states that failure to follow the code will result in disciplinary action that could include job termination.

Google also makes it clear that any unaddressed questions after reading the Code or any ethical issues must be reported to a manager, Human Resources, or Ethics & Compliance. Google also provides an Ethics & Compliance Hotline where questions and concerns of suspected violations can be raised. If the misconduct concern is with the CEO, a direct reporter to the CEO, or a Senior Vice President, the Code advises reaching out to the Audit Committee of Alphabet's Board of Directors and provides their address. Google has a strict no retaliation policy and instructs anyone who feels they have been retaliated against to contact the Ethics & Compliance department. These policies are in conjunction with the Seven Pillars' focus on communicating and training staff on how to handle issues, respond, and enforce the policies consistently.

Google's Code of Conduct outlines the organization's goals and provides additional details: serving our users, supporting and respecting each other, avoiding conflicts of interest, preserving confidentiality, protecting Google's assets, ensuring financial integrity and responsibility, and obeying the law. The Code makes it clear that Google wants to go above and beyond what the

[6] https://www.hipaajournal.com/is-google-drive-hipaa-compliant/
[7] https://abc.xyz/investor/other/google-code-of-conduct/

law requires. Without detailing processes and procedures for every possible scenario, Google's Code of Conduct embodies the Seven Pillars' focus on providing, communicating, and training on relevant processes and procedures. The Code establishes a culture of integrity that embodies the Code's letter and the spirit.

Google's Security Culture

Google's security culture drives their commitment to compliance. Google products' security controls are regularly externally audited and held to the national and international standards required by Google's certifications in addition to security standards that do not have required at certifications[8] presently. Google's security culture involves multiple tenets[9]: employee background checks, security training for all employees, internal security and privacy events, a dedicated security team, internal audit and compliance specialists, collaboration with the security research community, operational security, data access and restrictions, and encouraging users and administrators to go beyond compliance requirements. These methods show that Google is following the two foundations of compliance: due diligence and an ethical culture. Google's internal and external security demonstrates their due diligence and their insistence on going above and beyond legal requirements demonstrates their intent to create an ethical culture.

Google's compliance with the Seven Pillars is demonstrated through their implementation of a security culture. Google's employee background checks include education, previous employment, internal and external reference checks, criminal background check, credit check, immigration status check, and security checks. This works toward removing bad actors. If someone becomes a Google employee, they undergo security training as part of their orientation process, agree to the Code of Conduct, and have ongoing security training throughout their career as a Googler. This demonstrates Google's prioritization of processes and procedures that are communicated and trained on throughout Googlers' careers. Employees also receive more specific training depending on their role. For instance, security engineers focus on secure coding practices, product design, and automated vulnerability testing tools. Google also hosts regular internal events to raise awareness and employee engagement about security and privacy's importance. For instance, Google hosts "Privacy Week" across global offices to raise awareness of privacy issues all employees face. These initiatives allow Google to monitor, respond to, and enhance employees' understanding of security concepts.

Google also has more than 550 full time security and privacy professionals in addition to internal audit and compliance specialists. The internal audit team reviews and revises Google's compliance standards in light of the ever-changing security laws and regulations worldwide. Google also has independent external audits by third-parties. Google also connects with the broader research community through the Vulnerability Reward Problem. The program encourages researchers to report design and implementation issues they observe in Google's

---

[8] https://business.safety.google/compliance/

[9] https://static.googleusercontent.com/media/gsuite.google.com/en//files/google-apps-security-and-compliance-whitepaper.pdf

systems that may put customers' data at risk. Google provides financial awards with this program. Google's operational security involves vulnerability management through internal tools, malware prevention through encryption and third-party certificates, and data access and restrictions to keep Google's customers' data private. Google's above and beyond auditing efforts demonstrates their implementation of the auditing and monitoring pillar of compliance.

Google also encourages its clients to improve their security and compliance beyond the baseline Google's services provide. Google provides additional user features including authentication/authorization features such as two-step verification, Security Keys, secure single sign-on (SSO), Information Rights Management (IRM) for disabling downloading, printing and copying from the advanced sharing menu, additional email security, and increased data storage (even for deleted data).

Emerging Issues

Addressing HIPAA Compliance Issues

Google proactively addresses emerging HIPAA compliance issues. Google shares extensive information on compliance best practices and Google's compliance documentation such as security, third-party audits and certifications, documentation, and legal commitments to supporting compliance.[10] Google's products also undergo independent verification of their security, privacy, and compliance controls. This allows Google to achieve certifications, attestations of compliance, and audit reports comparing Google to other organizations worldwide. The third-party independent auditors examine Google's security practices, including data centers, infrastructure, and operations. HIPAA violations are expensive in many ways, especially the financial and reputational risks. Following the Seven Pillars' monitoring recommendation provides Google with revenue security so that profit is not lost in fines or lost business.

Audits and Certifications

Google implements the Seven Pillars' recommendation for monitoring by seeking guidance from leading standards and regulatory bodies to adjust their security and privacy programs as the compliance landscape changes. In addition to achieving compliance certifications, Google goes above and beyond by creating resource documents and mapping against frameworks and laws where formal certifications or attestations are not required.

The easy accessibility of Google's compliance certifications and their industry-leading standards where official certifications are not yet available, demonstrates Google's commitment to compliance. Some of Google's compliance certifications include[11]:

- The International Organization for Standardization (ISO) 27001 for security standards
- ISO 27017 for information security for cloud services

---

[10] https://workspace.google.com/learn-more/security/security-whitepaper/page-5.html

[11] https://cloud.google.com/security/compliance/hipaa

- ISO 27018 for personally identification information protection
- Service Organization Controls for evaluating an organization's system and controls for security, availability, processing information, confidentiality and privacy based on the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA)
- HITRUST CSF for nationally and internationally accepted security standards
- CSA STAR (Cloud Security Alliance's Security, Trust & Assurance Registry Program) for ensuring self-assessment, third-party audit, and continuous monitoring aiding in due diligence
- PCI DSS from the Security Standards Council for account data protection

Google's Security Culture

Google's tone from the top creates a security culture.[12] Security is imbued into Google's structure, technology, operations and approach to customer data. The Google Cloud Platform was built using a more than 700-person security engineering team. Google's robust security infrastructure and systems are the default for every Google client. This makes their base operations in compliance with global standards. Google also emphasizes going beyond the baseline standards and provides clients with opportunities to customize individual security settings through dashboards, account security wizards, access and authentication policies, single sign-on (SAML 2.0) features, OAuth 2.0 and OpenID Connect for authentication and authorization, Information Rights Management (IRM) resources, restricted email delivery, asset protection targeted toward email spam, phishing, email spoofing, and malware production. Google also recognizes clients' concerns regarding which Google employees have access to their HIPAA data. To assure clients, Google implemented administrative safeguards, vulnerability management, and threat monitoring under Google's Shared Responsibility Model.[13] The Shared Responsibility Model explains that Google and its clients share the responsibility of being compliant and keeping PHI secure. Google shares the responsibility with their clients so that the clients can focus more on their business than making sure their systems are secure. Although Google's clients are ultimately responsible for making sure they are being compliant, Google provides secure and compliant offerings. This places a significant portion of the cost of security and compliance onto Google and away from the client.

Administrative safeguards ensure that only a small group of Google employees have access to customer data. This access is determined based on their job functions and roles, using the guiding concepts of "least privilege" and "need-to-know basis." Google's commitment to transparency also includes providing clients with the ability to view logs showing when, how, and why Google employees accessed their data. Google's strong authentication programs design systems that only allow authorized persons to access data to ensure that personal data cannot be read, copied, altered, or removed without authorization from the client's administration. Google also makes sure that all employees, contractors, and sub-processors who have access to the customer data are under statutory obligation to confidentiality. These processes show Google's commitment to excluding bad actors by monitoring who has access to the data.

---

[12] https://workspace.google.com/learn-more/security/security-whitepaper/page-8.html
[13] https://services.google.com/fh/files/misc/google-cloud-platform-hipaa-overview-guide.pdf

Google's vulnerability management and threat monitoring involves using internal and external tools to scan for security threats automatically through manual penetration efforts, quality assurance processes, software security reviews, and external audits. If a security threat is determined by the systems, Google's vulnerability management teams research and address the threat. Google's internal monitoring and response systems provide a competitive advantage with compliance. Rather than waiting for a lawsuit or fines to address problems, Google creates in-house monitoring systems to continually address problems.

Risk Assessment

Business Associate Agreement (BAA)

Google's compliance program's continued risk assessments create risk management to limit Google's liability. For instance, Google's clients are tasked with determining if they are a HIPAA-covered entity, if they require a Business Associate Agreement (BAA) with Google, and ensure the environment and applications the company builds on top of Google Cloud's Platform are configured and secured according to HIPAA's requirements.

Google's requirement that clients who use a paid version of Google software sign a Business Associate Agreement[14] (BAA) creates an added layer of assurance that clients are HIPAA-compliant while using Google's products. The BAA is a contract stating that both entities are HIPAA-compliant and that each organization is responsible for their own compliance. If a client has not signed a BAA, they cannot use Google products for PHI.[15] Google's BAA limits clients' coverage to Google products specifically listed in the BAA, including[16]: Gmail, Calendar, Drive, Hangouts, Chat, Meets, Keep, Google Cloud Search, Voice, Sites, Groups, Jamboard, Cloud Identity Management, Tasks, and Vault.

Google Cloud Healthcare Data Protection Toolkit

Google also provides compliance resources to ensure clients are aware of Google's HIPAA compliance requirements and ways for the client to improve their compliance standards. Google provides the Google Cloud Healthcare Data Protection Toolkit[17] which is an automation framework for deploying Google Cloud resources to store and process healthcare data. It helps clients configure data storage, analytics, and application development. It also provides security and privacy best practice controls recommended for clients dealing with healthcare data (appropriate access, maintaining audit lots, monitoring suspicious activities).

The BAA and the Google Cloud Healthcare Data Protection Toolkit are two ways Google conducts due diligence. Since their clients are using Google's services while handling PHI, Google faces liability. Requiring that PHI clients sign the BAA stating that both their company and Google are

---

[14] https://compliancy-group.com/is-google-drive-hipaa-compliant/

[15] https://support.google.com/a/answer/3407054

[16] https://cloud.google.com/security/compliance/hipaa-guide

[17] https://cloud.google.com/architecture/setting-up-a-hipaa-aligned-project

HIPAA-compliant and responsible for their own compliance limits Google's exposure. Providing clients with the Google Cloud Healthcare Data Protection Toolkit ensures that clients are aware of their responsibilities since they are dealing with HIPAA data and they are aware of the services Google offers to enhance their protection of customer data.

If Google experiences a security breach, their compliance program will help mitigate the damages due to the two mitigating factors of the Federal Sentencing Guidelines for Organizations (FSGO). The first mitigating factor is whether or not Google had an effective compliance program that was consistent with the Seven Pillars at the time of the offense. Google's compliance program is upheld by the foundations of compliance (due diligence and an ethical culture) and the Seven Pillars. The program outlines clear processes and procedures that are overseen throughout the company. Bad actors are excluded due to extensive background checks. The program is communicated to employees during their orientation in addition to training throughout their time as a Googler. Google's focus on internal and external auditing provides monitoring for the program's effectiveness. In the event that a Google system finds a vulnerability, it will quickly be responded to, reported, and corrected.

The second mitigating factor deals with the organization self-reporting the offense to the appropriate government authority, cooperating in the investigation, and accepting responsibility for criminal wrongdoing. Google provided detailed instructions in the Code of Conduct regarding how employees should respond to a violation, which department they should report to, and resources for concealing their identity. Google's fulfillment of both mitigating factors gives the company a competitive difference. For instance, fulfilling the FSGO's mitigating factors decreases fines and punishments which would decrease the overall cost of the error and increase revenue overall.

Conclusion

Despite the complex HIPAA regulatory environment, Google's effective compliance program has provided their company and their clients with opportunities to improve the healthcare compliance landscape. It starts with the tone from the top security culture rooted in the Code of Conduct. Google is clear about who is bound by the Code and which processes and procedures they are responsible for. Google's staff is trained multiple times regarding the Code's procedures. Security risks surrounding Google's clients using HIPAA PHI data on Google services are carefully monitored by Google, Google's entire systems are monitored internally and externally through audits, and problems are rapidly addressed.

In addition to ensuring compliance, Google goes above and beyond to challenge themselves to improve the broader compliance environment by going beyond the required certifications and challenging their clients to also do so. The Business Associate Agreement (BAA) requirement and the Google Cloud Healthcare Data Protection Toolkit defend Google's interests. The BAA requirement ensures that all clients have stipulated to being in compliance with HIPAA regulations while they are using Google's systems for PHI. It also provides a clear outline of each party's responsibilities. Google's healthcare toolkit reminds clients of their HIPAA obligations in addition to offering extra services to go beyond the compliance baseline. Google's compliance program's effectiveness stems from its obedience of the Seven Pillars and the two foundations. The program's

effectiveness generates competitive differences for Google that increase revenue, improve the overall compliance landscape, and mitigate fallout from potential issues.