HIPAA and Zscaler: Compliance best practices for the cloud-first healthcare organization
Abstract

For enterprise IT strategists, the cloud promises scalability, flexibility, and ease of access. Like most industries, healthcare is moving to electronic records storage, analysis, and data delivery, and employing cloud-based technologies to manage and secure data. But the healthcare industry faces serious (and vertical-specific) challenges in protecting and securing electronic medical data in a cloud environment.

Healthcare providers must ensure the security and privacy of data in line within a stringent regulatory environment. The United States federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) governs the use, security, and management of private healthcare information, and its oversight impacts vendors across the entire healthcare spectrum.

But as those same providers migrate their data operations to the cloud, they face new cybersecurity challenges, in particular preserving compliance with HIPAA’s security and privacy provisions. In this paper, we examine how healthcare data operations based on a Secure Access Service Edge (SASE) cloud services architecture support and facilitate HIPAA compliance for healthcare providers.

Disclaimer: This white paper has been created by Zscaler for informational purposes only and is designed to try and help organizations understand HIPAA compliance in connection with Zscaler’s services and products. Therefore, it should not be relied upon as legal advice or to determine how the contents might apply to you or your organization. We encourage you to consult with your own legal advisor with respect to how the contents of this white paper may apply specifically to your organization, including your unique obligations under applicable law and regulations. ZSCALER MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS WHITE PAPER. This white paper is provided “as-is.” Information and views expressed in this white paper, including URL and other Internet website references, may change without notice. This document does not provide you with any legal rights to any intellectual property in any Zscaler product. You may copy and use this white paper for your internal, reference purposes only.

The history and (original) intent of HIPAA

Before HIPAA, the private U.S. health insurance industry was governed by different legal obligations, resulting in a patchwork of offerings. When it came to healthcare coverage, many insurance rights fell through cracks in the system. For example, when people lost or changed jobs, they often had reduced or missing insurance for pre-existing conditions.

In an effort to fill in coverage gaps, Congress and the White House worked on crafting new regulations. Part of this effort was finding a way for insurance providers to easily and securely share patient healthcare information—both physically and electronically. In 1996, Congress enacted and President Clinton signed HIPAA.

HIPAA was passed as part of a larger congressional healthcare reform attempt, originally introduced as the Kennedy-Kassebaum Act, and it contained two major objectives:

- Ensure individuals can keep their health insurance when changing jobs (health portability)
- Ensure the security and confidentiality of patient data and information, and set standards for the transmission and storage of data related to health care (administrative, financial, and health)

HIPAA requires that all health providers “adopt national standards for electronic healthcare transactions and code sets, unique health identifiers, and security.” But the drafters of the bill acknowledged a key threat to data integrity: “Congress recognized that advances in electronic technology could erode the privacy of health information.”

---

**PHI: What HIPAA aims to protect**

HIPAA governs industry use of individually-identified health information that relates to an individual’s past, present, or future physical or mental health condition or any other identifying information that can be used to identify the individual. HIPAA defines eighteen discrete identifiers of Protected Health Information, or PHI. Those identifiers include (but aren’t limited to):

- Name (full, or last name plus initial)
- Email Address
- Phone Number
- Social Security Number
- Device Identifier/Serial Number
- Web Uniform Resource Locators (URLs)
- Internet Protocol (IP) Number
- Biometric Identifiers
- Images

PHI constitutes sensitive and personal data related to the health of an individual. In the wrong hands, the data can be exploited. That threat risk demands a higher level of protection and regulatory oversight than is typically afforded to other types of data (e.g., industrial proprietary information or personal information not related to health care).

---

HIPAA's cloud-data tenets related to security and privacy

HIPAA Section II introduces five rules governing privacy, transactions and code sets, security, unique identifiers, and enforcement. Two relate to managing private healthcare data in the cloud: the Security Rule and the Privacy Rule.

**The Security Rule**, enacted in 2005, establishes national standards to protect the confidentiality, integrity, and availability of electronic PHI (ePHI). To comply, enterprises must implement policies and procedures to ensure the security of information systems that process, store, and transmit ePHI between entities:

- The **administrative section** sets security requirements for policies and procedures governing the development of technologies and administrative controls that protect access to ePHI. It outlines best-practice security management, responsibility, workforce, access, and contingency policies and procedures, among others.

- The **physical section** defines the procedures, policies, and standards for protecting the physical technologies that are used to process, store, or transmit ePHI. It defines policies for facility access, workstation use, device controls, and other physical systems and services.

- The **technical controls section** governs the policy and procedures of any technology that accesses, stores, modifies, or transmits ePHI, regulating access, audit, data integrity, and authentication procedures.

HIPAA's **Privacy Rule**—added in 2003—stipulates what information is considered PHI, and mandates that enterprises implement controls to prevent and restrict any unauthorized disclosure of PHI in any form (including paper or digital distribution). It requires organizations to protect PHI with appropriate safeguards that limit access to and use of the data. It also establishes how an enterprise can use PHI with (or without) explicit patient authorization.

The Privacy Rule clarifies the meaning of “privacy” with the “Minimum Necessary Rule.” The Minimum Necessary Rule determines how and when healthcare providers and other entities subject to HIPAA can disclose PHI. The Minimum Necessary Rule means that PHI can only be disclosed for a stated purpose.

---

The Privacy Rule also allows PHI to be used and disclosed for the purposes of treatment, payment, and healthcare operations. Otherwise PHI can only be disclosed in very narrow circumstances:

- When the disclosure is required by law, such as in the case of criminal activity or threat to a broader community
- When it is in the patient’s or the public’s interest: for instance, the routine delivery of patient services and care by HIPAA-covered entities that have a relationship with the patient might require disclosure of PHI
- When a HIPAA-covered entity needs a patient’s PHI from a different HIPAA-covered entity to provide services or coverage to the patient in question

Regardless of the circumstances, all covered entities must comply with the Minimum Necessary Rule.

The HIPAA mandate: Govern anything and anyone that touches PHI, anywhere, and at any time

HIPAA determines what information constitutes PHI, who can access PHI, when PHI can be accessed, how PHI can be used, and how PHI must be stored and transmitted in both electronic and physical form.

HIPAA applies to the following “covered entities”:

- Healthcare providers, including hospitals, clinics, laboratories, and individual doctors
- Healthcare data aggregators and clearing houses
- Health insurance and drug plan providers
- Health maintenance organizations (HMO)
- Some employers who provide a self-funded health care plan for their employees

Each of these organizations are required to comply with HIPAA and all of its associated regulatory standards. What is considered a “covered entity” under HIPAA occasionally changes. Updated information on which organizations are covered entities can be found on the CMS services website. 

---

HIPAA round 1.5: The HITECH Act

Recognizing new and growing digital transformation technologies, Congress enacted the Health Information Technology for Economic and Clinical Health (HITECH) Act in 2009. It updated HIPAA to cover new data technologies and fostered electronic health record (EHR) adoption. By 2017, HITECH helped enable 86% of office-based physicians to adopt EHRs and 96% of non-federal acute care hospitals to implement certified EHRs.8

The HITECH Act also imposed newer, stiffer penalties for healthcare companies that fail to comply with HIPAA’s privacy and security statutes.

Healthcare and digital transformation: more data in more places

Healthcare organizations strive to maintain user services and care while coping with ever-rising costs. New healthcare technologies such as cloud-based services (EHRs, genetic registries), and Internet-of-Things (IoT) devices (pacemakers, insulin pumps) can help healthcare organizations do more, better. For instance, facilitated access to patient data and real-time analytics of patient telemetry can contribute to better healthcare outcomes.

Digital transformation technologies like cloud and IoT are driving a huge increase in healthcare data volume: Data is not only cheaper to store and move, it’s easier to generate. Much of this data is stored and processed locally, but many healthcare services now store data in private data centers and private clouds. Cloud storage can introduce privacy concerns regarding data-sharing within an organization, with patients, or (when necessary) with third-party providers.

Sensitive PHI must remain secure as it is accessed, processed, stored, and moved between endpoints and authorized users. A critical need exists for secure technology infrastructure to protect access to PHI and EHRs in this new, distributed cloud environment. The cloud offers healthcare providers easier data management and access. The cloud also promises patients easier access as well, since patients now expect to access their data from smartphones, laptops, and home computers.

Healthcare providers’ embrace of cloud technologies enables them to deliver more consistent care and provide better information. But that information must now often travel via public internet connections, lengthening data travel distance, and extending a healthcare organization’s threat landscape. Healthcare companies that rely on legacy security technologies like hub-and-spoke networks and “castle-and-moat” security face a challenge: the further data travels, the more difficult it can be to secure. Data is potentially more exposed to breaches, malicious attacks, and increasing cybercrime. To take advantage of the cloud’s potential, healthcare providers must secure both access to data and the data itself (wherever it resides).

Planning for data-sharing under HIPAA: A disciplined, documented, defensible approach

HIPAA and (to an even greater extent) HITECH have accelerated healthcare industry adoption of digital PHI. HIPAA established rules governing Electronic Data Interchange (EDI), particularly with regard to data-sharing with third-party partners, defined in the legislation as “business associates.” Modern healthcare companies must follow a complex set of rules when it comes to data-sharing, and breach penalties can be severe. On top of that, HIPAA and HITECH mandate federal-level breach notification and reporting requirements for HIPAA-covered organizations and their business associates.

Yet despite all the details of and precedent set in HIPAA and HITECH, both pieces of legislation remain open to interpretation, particularly with regard to the management of data in the cloud. Unfortunately (and rather maddeningly), there is no formal certification authority or process for HIPAA compliance. And compliance gets complicated when it comes to storing PHI data in the cloud. Healthcare industry publication HIPAA Journal notes the risks:

“[T]here is no such thing as a HIPAA-compliant cloud drive as no cloud server can be truly HIPAA compliant. HIPAA compliance depends on the actions of the people. Even if appropriate security is used to secure data in the cloud, if healthcare organizations misconfigure settings or do not implement appropriate access controls, the HIPAA Security Rule could easily be violated.”

Ensuring enterprise compliance in that scenario is ultimately the responsibility of the healthcare services organization, and requires a disciplined, documented, and defensible approach. From that same HIPAA Journal article: “It is up to the covered entity to ensure policies and procedures are developed covering use of the cloud with respect to ePHI and that the cloud drive is configured correctly.”

For general PHI management related to HIPAA compliance, transparency is key. (Gartner Research prioritizes data discovery, ongoing compliance analysis, risk identification, and detailed risk mitigation.\(^\text{11}\))

All HIPAA-covered entities (including healthcare providers, services, and business associates) must create a HIPAA-compliant data-management plan. Such a plan should include the following features, among others:

1. Define and (more importantly) document how and where PHI data will be managed.
2. Establish, map, and audit dataflows (and supporting workflows) for PHI data, including its use with cloud providers (EHR, SaaS, etc.).
3. Establish a PHI-management risk profile, and audit operations (frequently) to measure risk against the profile.
5. Ensure decisions related to PHI data are both prudent and defensible.
6. For the sake of continuous improvement, regularly review HIPAA compliance planning with leadership and legal counsel.

“Define by service provided”: Designating cloud services under the HIPAA Security Rule

The HIPAA Security Rule was developed within the framework of technology and IT architectures existing at the time, long before the ubiquitous availability of cloud technologies. This complicates compliance for healthcare organizations that employ cloud services (which is most of them nowadays). How do you designate cloud service providers under HIPAA/HITECH? Covered entities? Business associates?

(HIPAA defines a “business associate” as “a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.”\(^\text{12}\))

\(^{11}\) Gartner Research "Q&A: Top Healthcare Provider HIPAA Inquiries", published 11 March 2019; Gregg Pessin, Sr. Director Analyst; https://www.gartner.com/document/3904377

Compounding matters, legacy security tools—e.g., so-called castle-and-moat firewall appliances—can be difficult to apply to a cloud environment. (How do you secure your corporate network perimeter when it extends to the unsecureable internet?)

Healthcare organizations may not be able to establish an “absolute” designation for a cloud-service provider. By HIPAA standards, the provider might be interpreted as a covered entity for one dataflow and as a business associate for another. Consequently, both the cloud provider and the healthcare enterprise (the covered entity, generally) must work together during deployment to ensure Secure Rule requirements are met as they relate to the service being provided.

Zscaler considerations under HIPAA

Per HIPAA, “covered entities” include health plans, healthcare clearinghouses, and healthcare providers that electronically transmit any health information for which the U.S. Department of Health and Human Services (HHS) has adopted standards. In addition, some employers that provide “self-funded” healthcare are considered covered entities under HIPAA.

Zscaler, as a cloud-security services provider in a healthcare environment, does not fall under an easily-identifiable HIPAA category. There are certain Zscaler deployment services (Sandboxing, DLP, and SSL) where Zscaler could be considered to have incidental access to customer-managed PHI. (This consideration depends on the services Zscaler provides to the covered entity, and on policies the customer applies.) In these (infrequent) cases, Zscaler can be considered a business associate, which may—on a case-by-case basis—require a supplemental customer business associate agreement (BAA). Note that any Zscaler BAA is by necessity limited in scope.

---

13 Ibid.

Zscaler and PHI: Adjust SSL, sandbox, and DLP for HIPAA compliance

In a healthcare-environment deployment, Zscaler services could incidentally access PHI in applying secure-socket-layer (SSL) traffic inspection, sandbox, and data loss prevention (DLP) services.

SSL inspection

SSL (and its successor TLS) is a data-encryption standard, and most internet data traffic is SSL/TLS-encrypted. According to Google, more than 93% of Chrome browser traffic is encrypted.15 (Zscaler worldwide data traffic is on average 83% encrypted.)

In a legacy security environment, encrypted traffic takes advantage of a blind spot: It bypasses security tools and policies, since inspection occurs between encryption on a source (perhaps malicious) server and decryption on a destination endpoint.

Zscaler’s SSL encryption/decryption feature16 decrypts, then inspects SSL-encrypted data traffic before it arrives. Zscaler then applies a customer’s security policies to that content. In this way, Zscaler intercepts, then blocks incoming threats, effectively reducing threat risk to the customer enterprise. The activity is—notably for the sake of HIPAA compliance—ephemeral: Zscaler does not preserve or record any of the source data (which in a healthcare environment could theoretically include PHI), only the policy metadata related to the customer’s security policy.

That distinction is subtle, and is not something explicitly called out in HIPAA language. SSL decryption is a necessary requirement to protect the enterprise: Threat actors encrypt malware to sneak it through security gateways. But it doesn’t get past Zscaler.

Bypassing SSL decryption is not generally recommended. But Zscaler’s SSL decryption brings Zscaler into incidental contact with PHI. For the sake of HIPAA compliance, healthcare organizations and other covered entities that employ Zscaler for SSL/TLS inspection can consider a workaround: Categorize the URLs of PHI-data locations and applications, and then set data traffic to/from only those URLs to bypass SSL inspection. In that way, a healthcare enterprise eliminates Zscaler’s incidental contact with PHI during decryption, and reduces risk of HIPAA non-compliance.

Bypassing SSL inspection—even if only for a small, PHI subset of data traffic—is a risk-based decision. Organizations must determine if the potential risk of HIPAA non-compliance with Zscaler SSL inspection exceeds the risk of a threat hiding in encrypted traffic entering the corporate network.

**Sandbox services**

Zscaler provides cloud-based advanced behavioral malware analysis services through its Cloud Sandbox service. Zscaler Cloud Sandbox\(^{17}\) enables customers to isolate suspicious files in a sandbox environment where they can be evaluated by Zscaler security: If the file is malicious, it is quarantined in a secure, encrypted data store. In rare cases, Zscaler ThreatLabZ security researchers may examine unique threat materials. If an infected file contains PHI, Zscaler may gain incidental access to PHI.

Zscaler maintains extensive access control requirements, storage, encryption, and logging for files that are accessed via Cloud Sandbox by the ThreatLabZ team. **Typically, Zscaler works with healthcare customers to gain insight or contextual understanding to identify PHI in relation to a covered entity's data. In that way, Zscaler and customer can take appropriate action to protect identified files containing PHI.**

To address HIPAA compliance with regard to Cloud Sandbox and PHI, covered entities can consider an alternative approach: categorize the URLs of PHI-data locations and applications, and then use that information to ensure PHI-inclusive files bypass the sandbox in transit. (This can be done via the "First Time Action = Allow & Do Not Scan" in Zscaler Cloud Sandbox rule policy.)

As with SSL inspection, bypassing sandboxing—even for a PHI subset of data traffic—is a risk-based decision. Organizations must measure the threat of missing an infected file against the risk of HIPAA non-compliance.

**Data Loss Prevention (DLP)**

Data Loss Prevention (DLP) is a Zscaler service that helps prevent the (intentional or unintentional) exfiltration of an enterprise's sensitive data.

Zscaler DLP\(^{18}\) examines dataflows. Zscaler sits inline between the user and the data destination, and uses dictionaries, content matching, file type control, machine-learning-based matching, and “Exact Data Match” to identify potential data exfiltration activity. In a healthcare setting, this service enables customers to detect and prevent sensitive medical data such as patient information, medical record numbers, disease names, drug names, lab reports from leaving control of the enterprise.

---


The Zscaler DLP solution provides actionable information to governance, risk, and compliance (GRC) systems and to security information and event management (SIEM) systems. It sends Internet Content Adaptation Protocol (ICAP) data to a centralized DLP system, and can alert DLP administrators via email. **Zscaler DLP can target or exempt specific users, groups, locations, destinations, and content types with granular multi-criteria policies.** Zscaler DLP does not store any sensitive data in logs or in the Zscaler cloud, and **all DLP processing is done in-memory.** Most HIPAA compliance programs include user education, and Zscaler alert notifications that provide users with sensitive data processing information help administrators understand HIPAA workflows.

Similar to SSL inspection and sandboxing, Zscaler DLP can—in examining data traffic—come into incidental contact with PHI. To reduce incidental access of PHI, Zscaler can provide healthcare customers with customized reports and notifications for visibility into DLP violations, as well as stream real-time log events to an external SIEM for further insights and correlation.

**Zscaler and HIPAA: The way covered entities achieve compliance**

Healthcare organizations employ cloud technologies to maximize services, minimize costs, and maximize efficiency. And though regulatory oversight—in the form of HIPAA and HITECH—has not always kept up with the pace of cloud-technology development, healthcare organizations can and should look to Zscaler to secure PHI digital transformation in a HIPAA/HITECH-compliant environment.

Zscaler delivers on the cloud’s promise of scalability, flexibility, and ease of access, and delivers those advantages securely. The Zscaler secure access service edge (SASE) architecture was designed in and for the cloud. With consideration to SSL inspection, sandboxing, and DLP, Zscaler can provide the cloud’s benefits and HIPAA compliance to progressive healthcare organizations.
About Zscaler

Zscaler was founded in 2008 on a simple but powerful concept: as applications move to the cloud, security needs to move there as well. Today, we are helping thousands of global organizations transform into cloud-enabled operations.