Solution Brief

HIPAA + Zscaler = Securing Healthcare

Patients | Organizations | Cybersecurity | Providers | Enterprises

How covered entities protect healthcare's CIA triad against cybercriminals with Zero Trust

Protect the security and confidentiality of patient data against cybercriminals with Zero Trust

Network security breaches lower our confidence in healthcare organizations, create chaos, and devastate patients' lives. One flaw in a hospital's cybersecurity armor can expose weak cybersecurity practices and sensitive patient data to those who prey and profit on our citizens and critical infrastructures.

During the first half of 2022, there were 337 data breaches impacting at least 500 records reported to the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR).[2] To make matters worse, IBM's annual Cost of a Data Breach report showed not only that the average cost of a healthcare data breach is now $10.1 million per incident—an increase of 9.4% increase from last year—but also that the Healthcare industry was the highest cost industry for the 12th year in a row. Moreover, IBM noted that critical infrastructure sectors, like healthcare, lagged in adopting Zero Trust strategies and cloud security best practices. Let's go into further detail:[3]

> "The healthcare field continues to be a top target for cybercriminals. According to data from the Department of Health and Human Services (HHS), there has been an 84% increase in the number of data breaches against healthcare organizations from 2018–2022 [...][1]"
>
> **Rick Pollack**
> President and CEO of the American

- **Critical Infrastructure Lags in Zero Trust:** Almost 80% of critical infrastructure organizations studied don't adopt zero trust strategies, seeing average breach costs rise to $5.4 million—a $1.17 million increase compared to those that do [adopt zero trust strategies].
- **Security Immaturity in Clouds:** 43% of studied organizations are in the early stages or have not started applying security practices across their cloud environments, observing over $660,000 on average in higher breach costs than studied organizations with mature security across their cloud environments.[4]

Lastly, IBM's report observed that organizations with mature cloud security infrastructures usually experienced lower data breach costs. Still, those in the early stages faced more challenges. Among other things, IBM Security recommended that organizations protect sensitive data in mature cloud environments and implement a Zero Trust Architecture (ZTA).

[1]Source: https://www.aha.org/news/perspective/2022-10-21-keeping-our-defenses-strong-against-cyber-threats
[2]Source: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
[3]Source: https://www.ibm.com/reports/data-breach
[4]Ibid

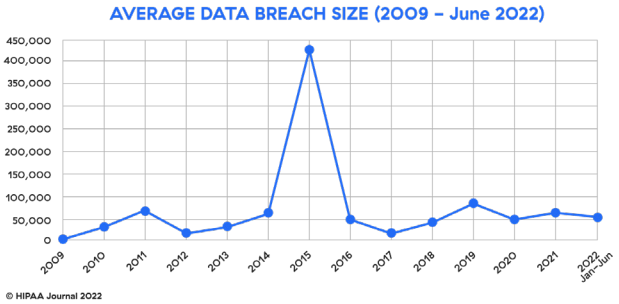
"But We've Always Done It That Way."

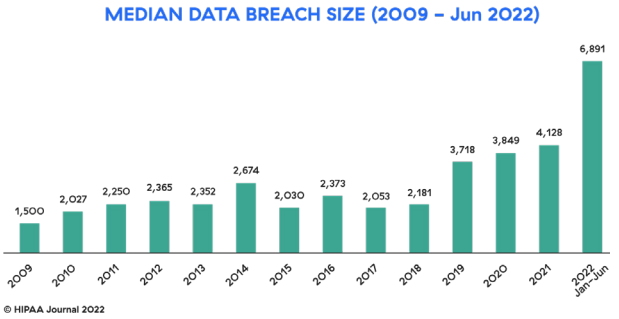
This is one of the most dangerous phrases in all of IT, let alone that of healthcare. Our IT systems and networks must be reliable, but stability should come neither at the cost of innovation nor on the heels of aging legacy architecture. Recently, the FBI's Cyber Division published a 'Private Industry Notification' warning the healthcare industry that "Medical device hardware often remains active for 10–30 years, however, underlying software life cycles are specified by the manufacturer, ranging from a couple [of] months to maximum life expectancy per device allowing cyber threat actors time to discover and exploit vulnerabilities."

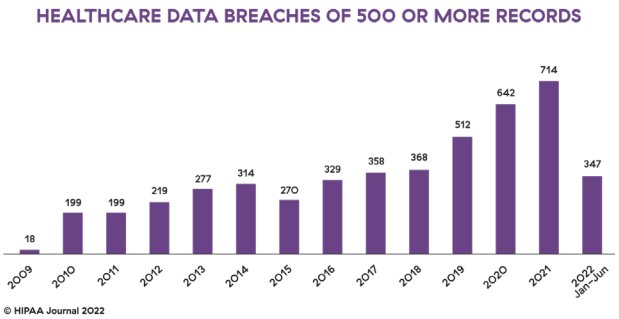
In a way, the FBI's statement is unsurprising. Traditional networks operating in an appliance-heavy manner increase the administrative burden and operational cost it takes to manage already hardware-bloated healthcare IT security.

Healthcare IT becomes even more challenging when migrating digital ecosystems to the mobile-first world, adopting bring your own device (BYOD), implementing telehealth, and incorporating the internet of medical things (IoMT), but still operating with a concentrated castle-and-moat architecture riddled with non-standardized policy misconfigurations.

This perspective focuses on internal security, but what about external threats? Trend Micro reports, "More than 36,000 healthcare-related devices in the US alone are easily discoverable on Shodan." With decentralized data, systems, and architectures, sensitive data, like protected health information (PHI), is vulnerable to attack. This adds up to an even taller order for healthcare organizations to reduce their attack surfaces and risk profiles and eliminate system access from cybercriminals.







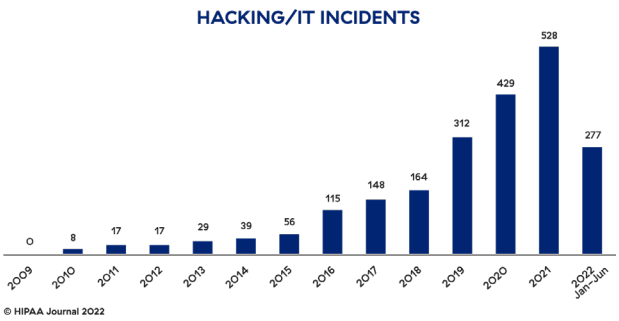
Escalation of Cyber Incidents

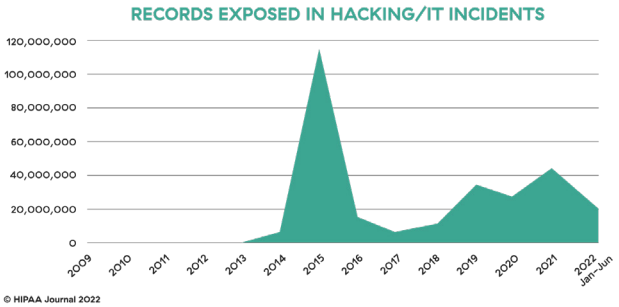
HIPAA Section II introduced five rules governing privacy, transactions and code sets, security, unique identifiers, and enforcement.

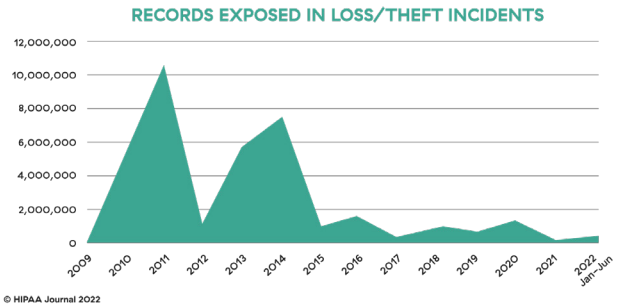
HIPAA's Security Rule[5], enacted in 2005, establishes national standards to protect the confidentiality, integrity, and availability of electronic PHI (e-PHI). To comply, enterprises must implement policies and procedures to ensure the security of information systems that process, store, and transmit e-PHI between entities. The Department of Human and Health Services summarizes safeguards corresponding to employing cloud technologies to safeguard e-PHI.[6] Despite the HHS's defined safeguards and standard operating procedures, policies, and templates, sophisticated cybercriminals have proven they're creative enough to ensure the healthcare industry remains under attack. This escalation of incidents is depicted in the HIPAA Journal's graphs.[7]

Administrative Safeguards

- **Security Management Process.**
  A covered entity must identify and analyze potential risks to e-PHI and implement security measures that reduce risks and vulnerabilities to a reasonable and appropriate level.
- **Information Access Management.**
  The Security Rule requires a covered entity to implement policies and procedures for authorizing access to e-PHI only with appropriate role-based access consistent with the Privacy Rule "minimum necessary" standard for using or disclosing PHI.
- **Evaluation.**
  A covered entity must perform a periodic assessment of how well its security policies and procedures meet the requirements of the Security Rule.







[5]Source: https://www.hhs.gov/hipaa/for- professionals/security/guidance/index.html
[6]Source: Respective to cloud technologies,
[7]Source: https://www.hipaajournal.com/healthcare-data-breach-statistics/

Physical Safeguards

- **Workstation and Device Security.**
  A covered entity must implement policies and procedures to specify the proper use of and access to workstations and electronic media. A covered entity must also have policies and procedures regarding the transfer, removal, disposal, and reuse of electronic media to ensure appropriate e-PHI protection.

Technical Safeguards

- **Access Control.**
  A covered entity must implement technical policies and procedures that allow only authorized persons to access e-PHI.
- **Audit Control.**
  A covered entity must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI.
- **Integrity Controls.**
  A covered entity must implement policies, procedures, and electronic measures to ensure that e-PHI is not improperly altered or destroyed.
- **Transmission Security.**
  A covered entity must implement technical security measures that guard against unauthorized access to e-PHI being transmitted over an electronic network.

HIPAA's Privacy Rule[8] provision—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, similar to zero trust's principle of least privilege, means that data can and should only be disclosed for a stated purpose and time period, especially PHI.

The Privacy Rule also allows PHI to be used and disclosed for treatment, payment, and healthcare operations. Otherwise, PHI is only disclosed when it is required by law, when it is in the patient's or the public's interest when HIPAA-covered entities need to exchange a patient's PHI between each other to provide services or coverage to the patient in question.

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

[8]Source: https://www.hhs.gov/hipaa/for- professionals/privacy/index.html

You Can't Prevent What You Can't Detect

Zscaler and HIPAA: How Covered Entities Achieve Compliance

Pre-COVID, healthcare organizations were already migrating their IT infrastructures to the cloud to secure PHI-rich environments despite HIPAA and HITECH not always keeping pace with technology. However, in the age of COVID, healthcare organizations expedited their digital transformation plans to promote telehealth and securely deploy cloud technologies to reduce operational costs and risks as well as increase their security profile in the most efficient way possible.

Zscaler's industry-leading cloud native Security Service Edge[9] (SSE) fulfills the cloud's promise of secure scalability, flexibility, and ease of access. Zscaler's Zero Trust Architecture (ZTA) provides the HIPAA-compliant cloud utility to progressive healthcare organizations, including threat protection, data loss prevention (DLP), SSL inspection, sandboxing, and much more. And because Zscaler connects users to applications, not IP networks, Zscaler enables aging health IT infrastructures to seamlessly leverage their current service catalog while adopting other cloud solutions. As noted in the HHS Office of Information Security[10], digital transformation, cloud technology adoption, and application and service migration to the cloud are shared responsibilities, so selecting the right SSE platform is the cornerstone of cloud security. Along with reducing cloud security risk and misconfiguration and improving compliance, shadow IT, and threat intelligence, **Zscaler enforces and supports the HHS OIC's best practices for securing a healthcare organization's cloud data.**

HHS Office of Information Security Top 10

1. Use a cloud service provider that encrypts
2. Conduct compliance audits
3. Implement a Zero Trust model
4. Set up your privacy settings
5. Use a Two-Factor Authentication
6. Establish and enforce security policies
7. Maintain cloud visibility
8. Understand cloud compliance, requirements, and regulations
9. Install updates to your operating system
10. Avoid using public Wi-Fi

[9]Source: https://www.gartner.com/doc/reprints?id=1-2966J3JL&ct=220218&st=sb
[10]Source: https://www.hhs.gov/sites/default/files/cloud-security-analyst-note-tlpwhite.pdf

Zscaler Internet Access (ZIA)

Zscaler's ZIA solution securely connects users to externally managed applications, including SaaS apps and internet destinations, regardless of device, location, or network. ZIA sits between users and the internet and ensures malware does not reach users and valuable corporate data does not leak out. It enforces access based on granular access control policies, inspects traffic, both unencrypted and encrypted, inline for malware and advanced threats, and prevents data leakage.

Policies follow users to provide identical protection on any device, regardless of location; any policy changes are enforced for users worldwide. The Zscaler cloud security platform provides full inline content inspection of webpages to assess and correlate the risk of webpage objects, continuously discovering and blocking sophisticated threats. ZIA includes broad functionality, which Zscaler categorizes into three areas: access control, threat prevention, and data protection.

1. Access Control

Zscaler's ZIA access control enforces access and usage policies to externally managed applications, including SaaS applications and internet destinations. This includes functionality traditionally provided by standalone point products, such as:

Cloud Firewall: The Zscaler Cloud Firewall was designed to protect users by inspecting internet traffic on ports and protocols. It offers user–level policies and application identification with deep packet inspection and intrusion prevention.

DNS Filtering: Zscaler's DNS filtering solution provides a local DNS resolver and enforces acceptable use policies.

URL Filtering: Zscaler's URL filtering capabilities enable customers to enforce acceptable usage policies and protect organizations from users visiting unauthorized websites or illegally downloading content that can increase liability and impact their brand.

Bandwidth Control: To improve productivity and user experience, Zscaler's bandwidth control and traffic shaping capabilities ensure that business–critical applications, especially proprietary healthcare applications, are prioritized over non–business–critical applications. By enforcing quality of service in the cloud, Zscaler's platform optimizes "last–mile" utilization of the health IT network, providing significant value.

2. Threat Prevention

Zscaler's second area of functionality, threat prevention, keeps users safe from savvy threat actors by providing multiple layers of protection. Zscaler provides functionality traditionally offered by disparate, standalone products, which are described below:

Advanced Threat Protection: Zscaler's advanced protection solution delivers real–time protection from malicious internet content like browser exploits, scripts, zero–pixel iFrames, malware, and botnet callbacks. Over 120,000 unique security updates are performed daily to the Zscaler cloud to protect users. Once Zscaler detects a new threat to a user, Zscaler will block it for every user.

Zscaler calls this the “cloud security effect.” Advanced threat protection features include:

SSL Inspection: SSL and TLS (SSL’s successor) are data encryption standards, and most internet traffic is SSL/TLS encrypted[11]. Google says more than 93% of Chrome browser traffic is encrypted. Similarly, Zscaler’s worldwide data traffic is, on average, 83% encrypted. Zscaler’s SSL encryption/decryption feature[12] decrypts and 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.

Botnet Protection: Protection from botnets that could be secretly installed on user devices to perform malicious tasks at the instruction of command-and-control servers.

Malicious activity content protection: Protection against websites that attempt to download dangerous content to a user’s web browser.

Fraud protection: Protection against phishing sites that mimic legitimate sites, such as banking and e-commerce sites, to steal confidential information.

Cross-site scripting (XSS) protection: Protection against XSS, in which malicious code injected into websites is downloaded to a user’s web browser from compromised web servers.

Suspicious destinations protection: Blocks requests to any country based on ISO 3166 mapping of countries to their IP address space. Websites are blocked based on the location of the web server.

Unauthorized communication protection: Protection against communications like internet relay chat (IRC) tunneling applications and “anonymizer” sites that are used to bypass firewall access and proxy security controls.

Peer-to-peer (P2P) anonymizer protection: Blocks anonymizing applications such as Tor, an application that enables users to bypass policies controlling what websites they may visit or internet resources they may access.

> “Google says more than 95% of Chrome browser traffic is encrypted. Similarly, Zscaler’s worldwide data traffic is, on average, 83% encrypted.

[11]Source: https://transparencyreport.google.com/https/overview?hl=en
[12]Source: https://www.zscaler.com/resources/white-papers/ encryption-privacy-data-protection.pdf

Sandbox: The Zscaler Sandbox enables enterprises to block zero day exploits and advanced persistent Threats (APTs) by analyzing unknown files for malicious behavior and can scale to every user regardless of location. Zscaler's purpose-built multitenant sandbox allows customers to determine which traffic should be sent to the Sandbox. As an integrated cloud security platform, healthcare IT administrators can set policies by users and destinations to prevent patient zero scenarios by holding, detonating, and analyzing suspicious files in the sandbox before being sent to the user.

Antivirus: Zscaler's antivirus technology uses a signature database of files and objects on the internet known to be unsafe and runs traffic through multiple antivirus engines in a single pass.

DNS Security: Zscaler blocks access to known malicious sites, including command-and-control sites, and routes suspicious traffic to Zscaler's threat detection engines for content inspection.

Browser Isolation™: Zscaler Browser Isolationl stops active content and ransomware from reaching endpoint devices and prevents the exfiltration of confidential data from business-critical applications.

3. Data Protection

Zscaler's data protection function prevents unauthorized sharing or exfiltration of confidential information, like e-PHI, reducing the health industry's HIPAA business and compliance risk.

Data Loss Prevention (DLP): Zscaler's DLP[13] service helps prevent intentional or unintentional exfiltration of an enterprise's sensitive data like PHI, HIPAA, PII, CUI, etc., and 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. Most HIPAA compliance programs include user education and Zscaler alert notifications that provide users with sensitive data processing information to help administrators understand HIPAA workflows.

Cloud Access Security Broker (CASB): Zscaler's CASB prevents data exposure, ensures SaaS compliance with out-of-band CASB, and discovers and controls unknown cloud applications with Inline CASB. Healthcare policies can be defined with granular access control for specified cloud applications, such as the ability to upload or download files or post comments or videos based on different user or group identities. Additionally, Zscaler partners with specific CASB vendors to extend their policy controls and visibility of out-of-band cloud applications.

Cloud Security Posture Management (CSPM): Zscaler's CSPM enables data security for any data type imported, stored, and exported during data collection, data analysis, remediations, single sign-on, and integrations. Data protection, high availability, and resiliency are considered as data and are replicated across multiple regions.

Browser Isolation: Zscaler's Browser Isolation

[13]Source: https://www.zscaler.com/products/data-loss-prevention

functionality allows customers to eliminate exposure to risky web content and data exfiltration by separating browsing activity from the end user device by isolating traffic to a secure cloud browser which can restrict the types of actions performed (e.g., download, read, write, etc.) on files from untrusted sources.

Zscaler Private Access

Zscaler's ZPA solution offers authorized users secure and fast access to internally managed applications hosted in enterprise data centers or the public cloud. Zscaler's ZPA solution's architecture does not expose applications' identity or location and only provides the necessary access levels. While traditional remote access solutions, such as virtual private networks (VPNs), connect a user to the corporate network, Zscaler's ZPA solution connects a specific user to a specific application without bringing the user onto the network, resulting in better security. Zscaler's ZPA solution was designed around Zscaler's key tenants that fundamentally change the way users access internal applications:

- Connect users to applications without bringing users onto the network.
- Never expose applications to the internet.
- Segment access to applications without relying on the traditional approach of network segmentation
- Provide remote access over the internet without VPNs

Zscaler's ZPA solution enforces a global policy engine that manages access to internally managed applications regardless of location. If access is granted to a user, Zscaler's ZPA solution connects the user's device only to the authorized application without exposing the identity or location of the application. Since applications are not exposed to the internet, the healthcare oranization's attack surface is eliminated, limiting threat exposure. This reduces cost and complexity while offering better security and an improved user experience. ZPA functionality falls within three major areas:

- **Secure Application Access:** Zscaler's ZPA solution delivers seamless connectivity to internally managed applications and assets, whether in the cloud, enterprise data center, or both. Healthcare IT administrators can set global policies from a single console, enabling policy–driven access that is network–agnostic to users. By creating access to applications regardless of a user's network, Zscaler's ZPA solution replaces the need for traditional remote access VPNs, SSL VPNs, reverse proxies, and other similar products.
- **Application Segmentation:** This architecture enables user and application–level segmentation capabilities. As each user–to–application connection is segmented with microtunnels, lateral movement across the network is prevented, significantly reducing unauthorized data access and security risk. Similar to CASB, ZPA's application discovery reports for internet applications and provides granular discovery of internally managed applications to aid the creation of segmentation policies, which ensure authenticated users are granted access only to authorized applications and not access to the IT infrastructure network.

Application Protection: Zscaler's ZPA solution

initiates and connects together outbound-only links between authenticated users and internally managed application microtunnels. Access is provided to users without bringing them onto the corporate network or exposing applications to the internet. Internally managed applications are not discoverable or identifiable. With no inbound connections and public IP addresses, there is no inbound attack surface, therefore removing the threat of distributed denial-of-service (DDoS) attacks. With Zscaler's approach, Zscaler subsumes the need for a next-generation firewall or DDoS mitigation system.

Zscaler HIPAA Considerations

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.[14] Also, some employers that provide "self-funded" healthcare are considered covered entities under HIPAA.

As a cloud security services provider in a healthcare environment, Zscaler does not fall under an easily discernible HIPAA category. There are certain Zscaler deployment services (sandboxing, DLP, and SSL) where Zscaler may have incidental access to customer managed PHI. This consideration depends on the services Zscaler provides to the covered entity and the policies the customer applies. In these rare 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, as Zscaler SSL traffic inspection, sandbox, and data loss prevention (DLP) services may incidentally access PHI in a healthcare environment.

- **SSL Inspection**

  This activity is—notably for the sake of HIPAA compliance—momentary, at best. Zscaler does not preserve or record any 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 requirement to protect the enterprise: Threat actors encrypt malware to sneak it through security gateways, but it doesn't get past Zscaler.

  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 noncompliance with Zscaler SSL inspection exceeds the risk of a threat hiding in encrypted traffic entering the corporate network. But Zscaler's SSL decryption brings Zscaler into incidental contact with PHI. For 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 the risk of HIPAA noncompliance.

- **Sandbox Services**

  In rare cases, Zscaler ThreatLabz security researchers may examine unique threat

[14]Source: https://www.hhs.gov/hipaa/ for-professionals/covered-entities/index.html

materials. If an infected file contains PHI, Zscaler may gain incidental access to PHI. Typically, Zscaler works with healthcare customers to gain insight or contextual understanding to identify PHI relating to a covered entity's data. In that way, Zscaler and the customer can take appropriate action to protect specified files containing PHI. Using Sandbox and PHI, covered entities can address HIPAA compliance using an alternative approach: categorize PHI–data URL locations and applications and then use that information to ensure PHI–inclusive files bypass the Sandbox in transit. (This is accomplished via the Zscaler Sandbox "First Time Action = Allow & Do Not Scan" 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 noncompliance.

- **Data Loss Prevention (DLP)**
  Zscaler DLP performs its processing in memory and does not store sensitive data in logs or within the Zscaler cloud. Most HIPAA compliance programs include user education and Zscaler alert notifications that provide users with sensitive data processing information to help administrators understand HIPAA workflows. Similar to SSL inspection and sandboxing, Zscaler DLP can—in examining data traffic—come into incidental contact

Zscaler's industry–leading cloud–native Security Service Edge[15]

(SSE) not only enforces and supports HIPAA's Security and Privacy Rules but fulfills the healthcare industry's requirements of reliability, availability, and scalability (RAS). And Zscaler accomplishes this feat in one of the most modern and secure ways possible: a zero trust architecture responsible for securing over 40 million concurrent users at any given time, including most US cabinet–level agencies.

[15]Source: https://www.gartner.com/doc/reprints?id=1–2966J3JL&ct=220218&st=sb

zscaler™ Healthcare Solutions | **The future of healthcare, secured.**

About Zscaler
Zscaler enables healthcare organizations and their strategic partners to securely transform their networks and applications, enabling the delivery of new care models and improving patient outcomes. Zscaler's HIPAA–compliant solutions ensure fast, secure connections between users and applications, regardless of device, location, or network. Zscaler operates the world's largest cloud security platform, protecting healthcare organizations across the globe from cyberattacks and data loss. Learn more at zscaler.com/industries/healthcare.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com