



# HIPAA + Zscaler = Securing Healthcare

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

Patients | Organizations | Cybersecurity | Providers | Enterprises

## 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 healthcare provider'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 2023, there were 395 data breaches impacting at least 500 records reported to the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR).<sup>1</sup>

To make matter worse, IBM's annual Cost of a Data Breach Report<sup>2</sup> indicates that since 2020, healthcare data breach costs have increased 53.3% and that, for the 13th year in a row, the healthcare industry reported the most expensive data breaches, at an average cost of USD 10.93 million.

The report also highlights that:

- **Cloud Environments are Frequent Targets**

82% breaches involved data stored in the cloud—public, private or multiple environments. Data breaches in public clouds and multiple environments also had higher costs.

- **Security System Complexity Matters**

The biggest data breach cost amplifier was identified as security system complexity. Organizations with high levels of security system complexity reported data breach costs 31.6% higher than those that with low or no security system complexity.

Building on their Zero Trust Architecture recommendation from last year's report, IBM designates modernizing data protection across the hybrid cloud as a key step organizations can take to prevent and reduce the cost of a data breach including:

- Working with data security and compliance technologies that work across all platforms.
- Deploying strong Identity and Access Management (IAM) strategies that include Multifactor Authentication.

**“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.<sup>3</sup>”**

—Rick Pollack  
President and CEO of the American

<sup>1</sup> [hipaajournal.com/july-2023-healthcare-data-breach-report/](https://hipaajournal.com/july-2023-healthcare-data-breach-report/)

<sup>2</sup> [ibm.com/reports/data-breach](https://ibm.com/reports/data-breach)

<sup>3</sup> [aha.org/news/perspective/2022-10-21-keeping-our-defenses-strong-against-cyber-threats](https://aha.org/news/perspective/2022-10-21-keeping-our-defenses-strong-against-cyber-threats)

## “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.

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.”

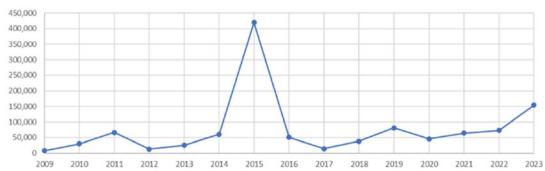
In a way, the FBI’s statement is unsurprising. Traditional networks operating in an appliance-heavy manner increase the administrative burden and operational cost it takes to manage already hardware-bloated healthcare IT security.

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.

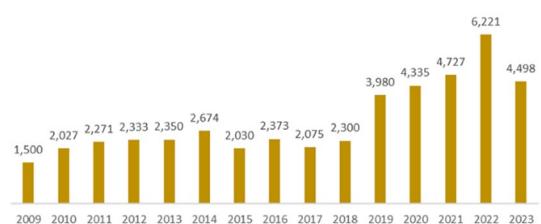
In its “2023 State of Cybersecurity for Medical Devices and Healthcare Systems”<sup>4</sup>, Health-ISAC found 993 vulnerabilities across 996 medical devices and health care applications, a 59% increase over 2022. With decentralized data, systems, and architectures, sensitive data, like

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.

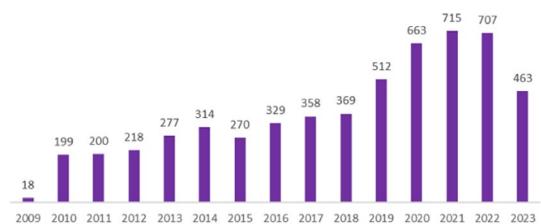
AVERAGE DATA BREACH SIZE (2009–AUG 2023)



MEDIAN DATA BREACH SIZE (2009–AUG 2023)



HEALTHCARE DATA BREACHES OF 500+ RECORDS (2009–AUG 2023)



<sup>4</sup> [h-isac.org/2023-state-of-cybersecurity-for-medical-devices-and-healthcare-systems/](https://h-isac.org/2023-state-of-cybersecurity-for-medical-devices-and-healthcare-systems/)

## 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<sup>5</sup>**, enacted in 2005, establishes national standards to protect the confidentiality, integrity, and availability of electronic Personal Health Information (e-PHI). To comply, enterprises must implement policies and procedures to ensure the security of information systems that process, store, and transmit electronic PHI between entities. The Department of Human and Health Services summarizes safeguards corresponding to employing cloud technologies to safeguard e-PHI.<sup>6</sup> 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.<sup>7</sup>

### 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.

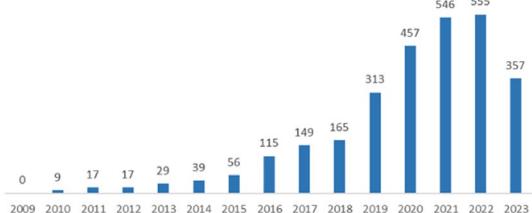
- **Information Access Management.**

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 e-PHI.

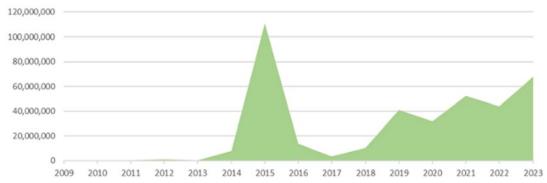
- **Evaluation**

A Covered Entity must perform a periodic assessment of how well its security policies and procedures meet the requirements of the Security Rule.

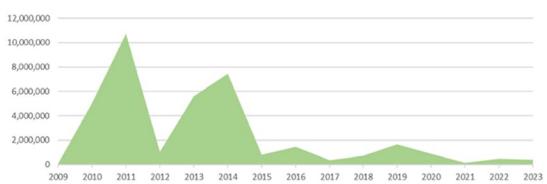
HACKING/IT INCIDENTS (2009–AUG 2023)



RECORDS EXPOSED IN HACKING/IT INCIDENTS (2009–AUG 2023)



RECORDS EXPOSED IN LOSS/THEFT INCIDENTS (2009–AUG 2023)



<sup>5</sup> [hhs.gov/hipaa/for-professionals/security/guidance/index.html](https://hhs.gov/hipaa/for-professionals/security/guidance/index.html)

<sup>6</sup> Respective to cloud technologies

<sup>7</sup> [hipaajournal.com/healthcare-data-breach-statistics/](https://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<sup>8</sup>** 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 certain 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.

<sup>8</sup> [hhs.gov/hipaa/for-professionals/privacy/index.html](https://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<sup>9</sup> (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, browser isolation and much more. And because Zscaler connects users to applications, not IP networks, Zscaler enables aging healthcare IT infrastructures to seamlessly leverage their current service catalog while adopting other cloud solutions. As noted in the HHS Office of Information Security<sup>10</sup>, 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

<sup>9</sup> [gartner-magic-quadrant-security-service-edge-sse-2023](https://www.gartner.com/magic-quadrant-security-service-edge-sse-2023)

<sup>10</sup> [hhs.gov/sites/default/files/cloud-security-analyst-note-tlpwhite.pdf](https://hhs.gov/sites/default/files/cloud-security-analyst-note-tlpwhite.pdf)

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

**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 Zscaler user, this is the "cloud security effect." Advanced threat protection features include:

**SSL Inspection:** In a legacy security environment, encrypted traffic creates a blind spot for security and compliance. SSL and TLS (SSL's successor) are data encryption standards, and most internet traffic is SSL/TLS encrypted. For example, Google says more than 95% of Chrome browser traffic is encrypted.<sup>11</sup>

Zscaler's SSL Inspection feature<sup>12</sup> decrypts, inspects, and then re-encrypts data traffic before it reaches its destination. This lets Zscaler intercept, identify and block incoming threats or apply customer data protection policies to reduce risks.

**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.

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

**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.

**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.

<sup>11</sup> [transparencyreport.google.com/https/overview?hl=en](https://transparencyreport.google.com/https/overview?hl=en)

<sup>12</sup> [zscaler.com/resources/white-papers/encryption-privacy-data-protection.pdf](https://zscaler.com/resources/white-papers/encryption-privacy-data-protection.pdf)

**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 Isolation 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<sup>13</sup> service helps prevent intentional or unintentional exfiltration of an enterprise's sensitive data like PHI and examines data flows. 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 to scan, detect and control PHI at rest in SaaS applications or to implement granular access control for specified cloud applications, such as the ability to upload or download files or post comments or videos based on user or group identities. Additionally, Zscaler partners with specific CASB vendors to extend their policy controls and visibility of cloud applications.

### Data Security Posture Management (DSPM):

DSPM proactively identifies and remediates misconfigurations in IaaS and PaaS to reduce risk, ensure compliance across AWS, Azure, and GCP, and maintain a sound security posture. With pre-built policies for compliance standards and security best practices, it helps security teams enforce guardrails for secure, compliant deployments that improve DevOps efficiency.

**Browser Isolation:** Zscaler's Browser Isolation 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.

<sup>13</sup> [zscaler.com/products/data-loss-prevention](https://zscaler.com/products/data-loss-prevention)

## 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 organization'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.<sup>14</sup> Also, some employers that provide “self-funded” healthcare are considered covered entities under HIPAA.

As a cloud security services provider, Zscaler does not fall under an easily discernible HIPAA category as it is not a Covered Entity, and rarely acts as Business Associate since it typically does not have access to, nor process PHI in most deployments. However, Zscaler services could access and/or process PHI in applying SSL Inspection, Sandbox, DLP, and Browser Isolation services, which may qualify Zscaler as a Business Associate.

Considerations depend on the services Zscaler provides to the Covered Entity and the policies the customer applies. In these rare cases, a supplemental customer Business Associate Agreement (BAA) may be required. Note that any Zscaler BAA is limited in scope to cover only those Zscaler products that may have access to PHI in a customer environment as described above.

### SSL Inspection

To enable detection of threats and enforce customer data protection policies, Zscaler decrypts SSL (or TLS) encrypted traffic according to customer defined configurations.

This activity is— notably for HIPAA compliance—ephemeral, performed entirely in memory, for the purpose of enabling other threat prevention and data protection services.

Bypassing SSL decryption is not generally recommended, but Zscaler’s SSL decryption can bring Zscaler into contact with PHI. To reduce the impact and to address HIPAA compliance, healthcare organizations and other covered entities that employ Zscaler for SSL 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 minimizes Zscaler’s contact with PHI during decryption.

### Sandbox Services

Zscaler provides cloud-based advanced behavioral malware analysis services through its Cloud Sandbox service.

Zscaler Cloud Sandbox enables customers to isolate suspicious files in an in-memory sandbox environment where they can be evaluated by Zscaler security. Only if the file is malicious will it be stored in a secure, encrypted location in the region chosen by the customer (United States or European Union). In rare cases, Zscaler ThreatLabZ security researchers may examine unique threat materials. If an infected file contains PHI, Zscaler may gain 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.

<sup>14</sup> [hhs.gov/hipaa/for-professionals/covered-entities/index.html](https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html)

To address HIPAA compliance regarding 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.)

### **Data Loss Prevention (DLP)**

Zscaler DLP can examine data at rest and data in motion. In a healthcare setting, this enables customers to detect and prevent sensitive medical data such as patient information, medical record numbers, disease names, drug names, and even lab reports from leaving control of the organization.

All Zscaler DLP processing is done in-memory and does not store any source data in logs or in the Zscaler cloud. Only the event metadata related to the customer’s security policy is logged. Zscaler DLP can also send Internet Content Adaptation Protocol (ICAP) data, including source data evidence, to an external DLP system or a Zscaler Incident Receiver in the customer environment, and can alert DLP administrators via email.

Zscaler DLP can—in examining data—come into contact with PHI. However, customer can define granular multi-criteria DLP policies that target or exempt specific users, groups, locations, destinations, and content types with granular multi-criteria policies. To help further reduce access of PHI, Zscaler can provide healthcare customers with customized reports and notifications for visibility into PHI activity.

### **Cloud Browser Isolation**

Cloud Browser Isolation (CBI) safely isolates users and endpoints from potential dangerous active web content and isolates customer private applications from unmanaged endpoints by rerouting web traffic through an isolated browser run by Zscaler.

When a user gets rerouted through CBI, they will continue to have the same experience within their local browser, but they will only see and interact with the image or pixel representation of the isolated browser session. Their local browser will no longer be exposed to active web content now running on the isolated browser, and customers can define policies for file upload or download through CBI.

Zscaler CBI can — in rendering web content — come into contact with PHI. User session content in memory or ephemeral storage within the isolation browser container is deleted as soon as the user’s session ends or crashes. Files that are uploaded/downloaded (as allowed by policy) or rendered (e.g., pdf in the isolated browser are temporarily stored in encrypted form and get deleted once the user action or session ends. The CBI service can also optionally persist user cookies in encrypted form to enhance user experience.

To reduce PHI exposure to the CBI service, customers can target or exempt specific users, groups, locations, destinations, and content types with granular multi-criteria policies. Customers can also disable Cookie persistence. CBI does not otherwise store any customer data in logs or in the Zscaler cloud.

## Zscaler's industry-leading cloud-native Security Service Edge<sup>15</sup>

(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.

<sup>15</sup> gartner-magic-quadrant-security-service-edge-sse-2023



Experience your world, secured.<sup>™</sup>

### About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at [zscaler.com](https://zscaler.com) or follow us on Twitter @zscaler.

+1 408.533.0288

Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134

[zscaler.com](https://zscaler.com)



© 2024 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ and other trademarks listed at [zscaler.com/legal/trademarks](https://zscaler.com/legal/trademarks) are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.