SOLUTION BRIEF

zentry security

HIPAA Compliance with Zero Trust Network Access

Best practices to maximize HIPAA compliance readiness

Risks

2020 saw **642 large healthcare data breaches** with more than **29M records disclosed.**[1]

In late 2020, the New Haven (Conn.) **Health Department agreed to pay over $200,000 for a 2017 HIPAA breach** related to a terminated **employee's continued access to patient records**.[2]

In 2018 the FBI discovered a server of a Tennessee-based healthcare service that **allowed anyone to search and view over 300,000 personal health records.**[3]

Best Practices

Implement Policies

Implement application-specific policies for employees, contractors, and third parties who have access to personal health information (PHI).

Deploy MFA

Deploy multi-factor authentication (MFA) to ensure only authorized users obtain access to sensitive PHI.

Log Access

Log all access activity to establish which users accessed specific records and when they did so.

Enable SSO

Enable single sign-on (SSO) to reduce the possibility of stolen credentials and prevent repetitive authentication.

This Solution Brief addresses how Zentry Security can help organizations adhere to these best practices to meet their HIPAA compliance requirements.

[1] HIPAA Journal, https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/
[2] Becker's Hospital Review, https://www.beckershospitalreview.com/cybersecurity/connecticut-city-pays-202k-hipaa-fine-for-failing-to-terminate-former-health-department-employee-s-phi-access
[3] Providertech, https://www.providertech.com/disastrous-hipaa-violation-cases-7-cases-to-learn-from/

HIPAA, The Health Insurance Portability and Accountability Act, requires healthcare organizations to implement precautions ensuring the security of their networks and the privacy of patient data. But, in a world of contractors, partners, clinicians, and patients all requiring access to PHI, this is clearly easier said than done.

It is sobering to view the number of breaches reported by the Office of Civil Rights (OCR) of the U.S. Department of Health and Human Services. From January 1 to mid-April 2021, nearly 150 breaches occurred, each of which affected hundreds to over half a million individuals. Most are due to "unauthorized access/disclosure" or "hacking/IT incident." [4]

Possibly more sobering, however, is that the vast majority of incidents could be addressed by implementing zero trust secure access methods. Granular policy enforcement and multi-factor authentication are just two examples that increase HIPAA compliance by restricting PHI access to authorized personnel. Employing such techniques significantly reduces the possibility of data exfiltration while helping meet HIPAA compliance requirements and streamlining the process of accessing PHI records on-premises or in the cloud.

Zentry Trusted Access

Zentry Trusted Access (ZTNA) provides secure zero trust application access for small- to medium-sized enterprises through a unified platform, which includes client and clientless approaches, to optimize the customer experience, ease administration, and increase security posture. The solution increases an organization's security profile and helps meet compliance obligations such as HIPAA. It also provides greater visibility into users and applications, and can be rapidly deployed, configured, and managed.

HIPAA Administrative & Technical Safeguards

HIPAA sections 164.308 and 164.312 requires healthcare organizations to implement or address policies and procedures for electronic systems to secure access to PHI. The tables below provide recommendations and guidance for each section.

[4] OCR Breach Portal, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Section 164.308 – Administrative Safeguards

IMPLEMENTATION SPECIFICATIONS	RECOMMENDATIONS
164.308(a)(1)(ii)(D) **Information system activity review** "Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports."	Routinely check log-ins and log-in attempts by reviewing Zentry Trusted Access logs for better insight into user behavior, access requests, and application usage.
164.308(a)(3)(ii)(A) **Workforce Security** "Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed."	Zentry Trusted Access policies can be used to restrict access to specific applications and resources. Such policies will, by default, prevent unauthorized users from accessing applications with sensitive PHI.
164.308(a)(3)(ii)(C) **Termination Procedures** "Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section."	As noted immediately above, Zentry's policies can be used to restrict access to applications. A policy can simply be edited to remove a specific user from accessing one or more applications that contain PHI.
164.308(a)(4)(ii)(B) **Access Authorization** "Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism."	Zentry Trusted Access leverages MFA to ensure only authorized users obtain access to sensitive information.
164.308(a)(5)(ii)(C) **Log-in monitoring** "Procedures for monitoring log-in attempts and reporting discrepancies."	Zentry's log files contain detailed information about user access to applications, including information about when an application was accessed. Zentry's dashboards also give a quick view of successful and failed log-in attempts.

Section 164.312 – Technical Safeguards

IMPLEMENTATION SPECIFICATIONS	RECOMMENDATIONS
164.312(a)(2)(i) **Unique User Identification** "Assign a unique name and/or number for identifying and tracking user identity."	Zentry Trusted Access can be integrated with user and device identity systems such as Microsoft AD, Okta, and others to enable user appropriate identity tracking.
164.312(a)(2)(iv) **Encryption and decryption** "Implement a mechanism to encrypt and decrypt electronic protected health information."	Zentry Trusted Access encrypts all sessions end-to-end with TLS, ensuring that all sensitive information is secure while in transit.
164.312(b) **Audit controls** "Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."	Zentry maintains logs of all application and resource access, both successful and unsuccessful. This information can be reviewed periodically to maintain compliance.
164.312(d) **Person or entity authentication** "Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed."	Zentry Trusted Access implements MFA to ensure that users are fully authenticated and authorized to access PHI. Moreover, Zentry integrates with identity systems such as Microsoft AD and other PKI infrastructure to confirm the identities of people requesting access to PHI.
164.312(e) **Transmission security** "Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network."	Zentry Trusted Access encrypts all sessions end-to-end with TLS, ensuring that all sensitive information is secure while in transit.

Conclusion

Today, healthcare organizations are under increasing stress from digital transformation, compliance mandates, and even a pandemic. Further, healthcare is targeted four times more than other industries by attackers and threat actors, with the average breach costing over $7M.[5] HIPAA fines can spiral to $1.5M per violation per year, not to mention patient loss, possible credit monitoring for affected individuals, breach notification costs, and legal fees.[6]

Regulations, like HIPAA, apply to organizations of all sizes in industries as diverse as healthcare, financial, manufacturing, and government sectors. Zentry's modern, zero trust secure access solution enables only authorized users to access specific applications and resources in the cloud and data center while reducing the overall attack surface, helping organizations meet stringent compliance requirements and mandates.

By implementing zero trust secure access solutions like Zentry Trusted Access, healthcare organizations can better meet their compliance requirements and increase their overall security profile.

[5] IBM Security, Cost of a Data Breach Report 2020
[6] HIPAA Journal, January 2021

Zentry Security provides next-generation secure access solutions that improve security, productivity, visibility, and usability. Zentry empowers modern enterprises by delivering zero trust secure access from any device to any application or resource located on-premises or in the cloud.

Learn more at **www.zentrysecurity.com**

zentry™ security

Zentry Security, Inc, 1371 McCarthy Blvd., Milpitas, CA 95035

E : info@zentrysecurity.com **T :** 1.866.4.ZENTRY
W : www.zentrysecurity.com **F :** 408.240.8754