HIPAA Security Rule Updates & IAM Compliance Recommendations

To comment on this article, please visit our GitHub repository and submit an issue.

Table of Contents

HIPAA SECURITY RULE UPDATES & IAM COMPLIANCE RECOMMENDATIONS 1

- **ABSTRACT** 1
- **INTRODUCTION TO HIPAA** 2
- **TERMINOLOGY** 3
- **INTRODUCTION TO IDENTITY AND ACCESS MANAGEMENT (IAM)** 4
- **2024 UPDATED HIPAA SECURITY RULES REQUIREMENTS RELATED TO IAM** 4
  - ***Access Control (HIPAA Security Rule – § 164.312(a))*** *4*
  - ***Audit Controls (HIPAA Security Rule – § 164.312(b))*** *5*
  - ***Authentication and Password Policies (HIPAA Security Rule – § 164.312(d))*** *5*
  - ***Data Encryption (HIPAA Security Rule – § 164.312(a)(2)(iv))*** *5*
  - ***User Training and Awareness (HIPAA Security Rule – § 164.308(a)(5))*** *5*
  - ***Data Minimization and Least Privilege (HIPAA Security Rule – § 164.308(a)(4))*** *6*
  - ***Data Integrity (HIPAA Security Rule – § 164.312(c)(1))*** *6*
  - ***Physical and Logical Security (HIPAA Security Rule – § 164.310 and § 164.312)*** *6*
  - ***Implementing IAM in Compliance with HIPAA*** *6*
- **CHALLENGES AND BEST PRACTICES** 9
- **FUTURE TRENDS IN IAM AND HIPAA** 10
- **CONCLUSION** 12

SOURCES 12

AUTHOR BIOS 14

Abstract

This article provides a comprehensive overview of the Health Insurance Portability and Accountability Act (HIPAA) and the importance of Identity and Access Management (IAM) in ensuring compliance with the proposed HIPAA Security Rule updates for protecting the security and privacy of healthcare information. We also explore challenges, best practices, and latest trends of using IAM to secure health information and achieve HIPAA compliance.

Introduction to HIPAA

Passed in 1996, HIPAA is a U.S. federal law enacted to safeguard sensitive patient-protected health information (PHI). HIPAA establishes comprehensive standards for handling, storing, and transmitting PHI to ensure the privacy and security of medical records. These standards include the Privacy, Security, Breach Notification, and Enforcement Rules.

- Privacy Rule establishes national standards for safeguarding PHI, regulating how covered entities and their business associates use and disclose PHI.[1]
- Security Rule outlines the administrative, physical, and technical safeguards required to protect electronic PHI (ePHI) from unauthorized access or disclosure.[2]
- Breach Notification Rule requires covered entities and business associates to notify individuals and the HHS in the event of a breach of unsecured PHI.
- Enforcement Rule establishes the procedures for investigations, penalties, and enforcement of HIPAA rules. The Office of Civil Rights (OCR), a division of the Department of Health and Human Services (HHS), is responsible for enforcing HIPAA compliance.

Compliance with HIPAA is mandatory for covered entities[3], including healthcare providers, pharmacies, health plans (insurance providers), and healthcare clearinghouses, as well as their business associates. Violations, deliberate or accidental, can lead to fines and penalties ranging from $141 - $2,134,831 with the possibility of prison for 1 to 10 years, according to the law as of the time of this writing.[4]

The last major update to HIPAA was in 2013 when the HIPAA Omnibus Rule introduced new HIPAA regulations mandated by the Health Information Technology for Economic and Clinical Health (HITECH) Act; this amendment addressed challenges arising from electronic health records (EHR), helping HIPAA accomplish its principal objective: ensuring patients feel safe disclosing sensitive information with their healthcare provider while allowing that data to be shared for treatment, research, and public health needs.[5,6]

Since then, most HIPAA changes have consisted of amendments to existing standards to accommodate changes to other laws, Executive Orders, and new transaction code sets. On December 10, 2020, the HHS OCR issued a Notice of Proposed Rulemaking, which proposed a range of changes to the HIPAA Privacy Rule. The new federal administration is expected to release a final rule implementing these changes later in 2025.

In December 2024, the HHS OCR proposed a rule that will implement numerous changes to the HIPAA Security Rule (a major goal being the improvement of cybersecurity in alignment with the NIST framework in an all-up cybersecurity initiative to secure PHI). After delays, the proposed rule was added to the Federal Register[7] (a daily publication for the U.S. government to announce changes to government requirements and policies) on January 6, 2025. For the next 60 days, any person or group can submit a comment on any part of the proposed rule by clicking the green “Submit a Formal Comment” button on the rule’s page. These comments will be added to the public record and weighed alongside data and facts

presented for the final ruling on March 7, 2025; however, several lobbying groups are pushing for this not to go into effect[8], so the rule may get a last-minute pause.

Terminology

Term	Description
Business Associate	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.[12]
Covered Entity	Person, organization, or institution that transmits ePHI (e.g., healthcare providers, health plans, healthcare clearinghouses).[3]
DID	Decentralized identity is a system allowing users to manage their personal information without relying on a central authority.
ePHI	Electronic Protected Health Information
Healthcare Clearinghouse	A healthcare clearinghouse under HIPAA is defined as a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value added" networks and switches, that performs either of the following functions: (1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data HIPAA elements, or (2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.[12]
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
IAM	Identity and Access Management (IAM) is the discipline used to ensure the correct access is defined for the correct users to the correct resources for the correct reasons.[13]
MFA	An approach whereby a user's identity is validated to the trust level required according to a security policy for a resource being accessed using more than one factor (something you know (e.g., password), something you have (e.g., smartphone), something you are (e.g., fingerprint)[18]
NIST	National Institute of Standards and Technology
NIST Cybersecurity Framework	The NIST Cybersecurity Framework helps businesses of all sizes better understand, manage, and reduce their cybersecurity risk and protect their networks and data.[15]
NPRM	Notice of Proposed Rulemaking is the first public release of a proposed document explaining an agency's plan to create a new regulation or change an existing one.[14]
OTP	A one-time password is a security code valid for one transaction or login attempt.
PHI	Protected Health Information
RBAC	Role-Based Access Control is a security method restricting access to systems and resources based on a user's role within an organization.

SOD	Segregation of Duties is a principle preventing any one person from being solely responsible for an entire process – it involves assigning different tasks to multiple people, which reduces the risk of fraud or error.
Transaction Code Sets	Transaction code sets refer to a standardized collection of codes used to represent specific actions or events within a system, allowing for the electronic exchange of information between different entities in a consistent format. In healthcare, it ensures accurate data transmission through standardized codes for diagnoses and procedures.[16]
ZTA	Zero Trust Architecture is a cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero-trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero-trust architecture plan.[17]

Introduction to Identity and Access Management (IAM)

Identity and Access Management (IAM) is the discipline used to ensure the correct access is defined for the correct users to the correct resources for the correct reasons.[13] This helps to ensure that only the right people (or systems) have access to specific data, applications, and resources within an organization. Compromised user credentials are frequently targeted by hackers to infiltrate organizations' networks via malware, ransomware, and phishing attacks. IAM safeguards resources by performing authentication (the process of proving that the user with a digital identity who is requesting access is the rightful owner of that identity[13]) and authorization (determining a user's rights to access resources and the level at which that access should be granted[13]) actions.

This article will cover the proposed cybersecurity measures added to the HIPAA Security Rule and the required IAM safeguards organizations should implement.

2024 Updated HIPAA Security Rules Requirements Related to IAM

HIPAA guidelines for protecting the security and privacy of healthcare information came into effect in 2005[21]; IAM plays a crucial role in meeting HIPAA's Security Rules requirements, as it governs individuals' access to PHI and ensures only authorized users can interact with the data. Below are the 2024 proposed updates to HIPAA Security Rule requirements:

Access Control (HIPAA Security Rule – § 164.312(a))

The Access Control HIPAA Security Rule mandates that covered entities and business associates implement policies to ensure that only authorized individuals can access PHI. IAM platforms play a crucial role in controlling and managing access to sensitive data:

- **Unique User Identification:** Each user must have a unique ID to track and log access to PHI, such as an email address, employee ID, or similar unique identifier in the context of the covered entity.

- **Emergency Access Procedure:** Establishing Emergency access procedures to allow authorized personnel to access PHI in case of an emergency while maintaining security policies.
- **Access Authorization and Management:** Access must be granted based on job roles and responsibilities (e.g., a doctor might have full access to patient records, while a billing clerk might only access billing-related information).
- **Access Control Mechanisms:** Restricting access based on user roles.

Audit Controls (HIPAA Security Rule – § 164.312(b))

HIPAA now requires audit controls to monitor access to PHI. IAM systems are crucial for providing detailed logging and audit trails of which individual had access to data and when.

- **Audit Logging:** IAM systems must record all access to PHI, including user activity, successful and failed login attempts, and access to specific records.
- **Audit Reports:** Organizations must be able to generate reports from IAM systems that show user access patterns and potential breaches or anomalies. IAM systems must be capable of generating data, which is typically done through access and audit logs.
- **Monitoring and Response:** IAM systems must allow for the continuous monitoring of user activity and the ability for organizations to respond to suspicious or unauthorized access.

Authentication and Password Policies (HIPAA Security Rule – § 164.312(d))

Strong authentication is a vital component of IAM under HIPAA to ensure that only authorized individuals can access PHI.

- **Authentication Mechanisms:** Authentication must be implemented using methods such as strong passwords and MFA.
- **Password Complexity:** HIPAA doesn't specify exact password policies, but it does require entities to implement policies to ensure strong passwords.

Data Encryption (HIPAA Security Rule – § 164.312(a)(2)(iv))

Data encryption protects PHI at rest and in transit. IAM solutions can be used to ensure that data is not exposed to unauthorized users, even if access control measures are bypassed.

- **Encryption of PHI:** Access to encrypted data should require proper authentication, and the IAM system should control who has the decryption keys.
- **Access Control for Decryption:** Only authorized individuals should be allowed to access encryption keys.

User Training and Awareness (HIPAA Security Rule – § 164.308(a)(5))

Conducting training initiatives ensures users understand the importance of safeguarding PHI.

- **User Training:** Users should be regularly trained on security best practices.
- **Access Control Awareness:** Organizations should inform users about the consequences of unauthorized access.

Data Minimization and Least Privilege (HIPAA Security Rule – § 164.308(a)(4))

The principle of least privilege ensures access to the minimum amount of PHI necessary to perform their job duties, supporting separation of duties.[9]

- IAM systems need to enforce the principle of least privilege by assigning users access based on their roles.
- Access permissions should be reviewed regularly to ensure that users no longer have access to data they no longer need for their job functions.

Data Integrity (HIPAA Security Rule – § 164.312(c)(1))

Ensuring the integrity of PHI is vital; IAM systems must be designed to prevent unauthorized changes to PHI and monitor for any alterations.

- Only authorized users should have permission to modify PHI. IAM systems should restrict this based on user roles and responsibilities.
- Any changes to PHI should be logged, tracked, and auditable through IAM tools.

Physical and Logical Security (HIPAA Security Rule – § 164.310 and § 164.312)

Though IAM primarily addresses logical access, it also interacts with physical security measures; both physical and logical security should be aligned to prevent unauthorized access to systems containing PHI.

- IAM systems should integrate with physical access control mechanisms, such as smartcards or biometric systems, to prevent unauthorized physical access to facilities where PHI is stored.
- IAM should ensure that remote access to PHI is secure.

Implementing IAM in Compliance with HIPAA

Below is a step-by-step guide on IAM updates required by the proposed updates in the HIPAA Security Rule:

HIPAA Security Rule	Definition	IAM Recommendation
Access Control	• Unique User Identification: Each user must have a unique ID to track and log access to PHI. • Emergency Access Procedure: Establishing Emergency access procedures to allow authorized personnel to access PHI in case of an emergency while maintaining security policies.	• **Assigning a unique ID** ensures individuals are uniquely accountable for their actions while cutting down on sharing credentials and preventing/limiting simultaneous logons. • **Create two or more emergency access accounts** for break-glass scenarios, granting authorized personnel immediate access to critical systems or data during an emergency. Define clear policies and procedures outlining conditions under which emergency access can be granted, who is authorized to request and approve it, and specific steps to follow. Make sure to

(HIPAA Security Rule – § 164.312(a))	• Access Authorization and Management: Access must be granted based on job roles and responsibilities (e.g., a doctor might have full access to patient records, while a billing clerk might only access billing-related information). • Access Control Mechanisms: Restricting access based on user roles.	implement MFA to verify the identity of critical personnel and ensure all emergency activities are monitored and logged. • **Regulate resource access using Role-Based Access Control (RBAC)**, which governs systems and data access by associating permissions with individual organizational roles (tailored to reflect the user's hierarchical position and department). RBAC operates on the principle of least privilege and makes sure each user is granted only the minimum permissions necessary for their job functions. • **Run Privileged User Access Reviews** to ensure users with elevated access (e.g., sensitive data or critical systems) possess only necessary and appropriate access levels. • **Establish policy enforcement points** to institute compliance with your access control policies.
Audit Controls (HIPAA Security Rule – § 164.312(b))	• Audit Logging: IAM systems must record all access to PHI, including user activity, successful and failed login attempts, and access to specific records. • Audit Reports: Organizations must be able to generate reports from IAM systems that show user access patterns and potential breaches or anomalies. • Monitoring and Response: IAM systems must allow for the continuous monitoring of user activity and the ability for organizations to respond to suspicious or unauthorized access.	• **Set up audit logging** with your Identity Provider – these logs capture every logged event (e.g., changes to applications/groups/users, sign-ins, etc.). • With audit logging and access control policies in place, organizations can easily pull **audit reports** from their IAM system, flagging resources users have access to alongside risky/anomalous activity. • **Regular audits and reviews** continually monitor your IAM system and make necessary improvements to respond to gaps, changes, and emerging risks. Such monitoring and response capabilities are included with most Identity Provider service packages. • **Set up threat detections, alerts, and mechanisms during monitoring** to ensure there is remediation of any logs not stored or missing and required.
Authentication and Password Policies (HIPAA Security Rule – § 164.312(d))	• Authentication Mechanisms: Authentication must be implemented using methods such as strong passwords, • Password Complexity: HIPAA doesn't specify exact password policies, but it	• **Requiring MFA** adds an extra layer of security, ensuring users provide sign-in credentials and a one-time password (OTP) or a cryptographically verified and generated string from a hardware device. • **Phishing-resistant MFA**, authentication mechanisms that are inherently resistant to phishing attacks, ensures that even if a

	does require entities to implement policies to ensure strong passwords.	user is tricked into divulging their credentials, attackers cannot use them to access sensitive systems or data. • **Create password policies** to enforce minimum password lengths and password complexity rules to make passwords stronger and more difficult to guess. • **Audit and rotate credentials periodically** to limit how long these credentials have access to certain resources.
Data Encryption **(HIPAA Security Rule –** **§ 164.312(a)(2)(iv))**	• Encryption of PHI: Access to encrypted data should require proper authentication, and the IAM system should control who has the decryption keys. • Access Control for Decryption: Only authorized individuals should be allowed to access encryption keys.	• **Implementing a key management service** (KMS) helps prevent unauthorized access to encrypted data by making sure keys are handled securely throughout their lifecycle. These services also help control who can manage keys separately from who can use them, in addition to auditing who used which keys, when, and on which resources. • Utilizing **hardware security modules (HSM)** devices provides tamper-resistant hardware that secures cryptographic processes by generating, protecting, and managing keys used for encrypting and decrypting data and creating digital signatures and certificates.
User Training and Awareness **(HIPAA Security Rule –** **§ 164.308(a)(5))**	• User Training: Users should be regularly trained on security best practices. • Access Control Awareness: Organizations should inform users about the consequences of unauthorized access.	• Educate users and administrators on IAM security best practices. Everyone should be aware of their roles and responsibilities, as well as the potential threats and consequences of IAM misuse. Provide regular training for employees/vendors and test their knowledge.
Data Minimization and Least Privilege **(HIPAA Security Rule –** **§ 164.308(a)(4))**	• IAM systems need to enforce the principle of least privilege by assigning users access based on their roles. • Access permissions should be reviewed regularly to ensure that users no longer have access to data they no longer need for their job functions.	• Implementing a larger **Identity Governance** solution would automatically ensure the right people have the right access to the right resources, with identity and access process automation, delegation to business groups, and increased visibility. For example, lifecycle workflows and entitlement management can automatically add and remove users into groups or access packages so that access to applications and resources is updated. Users can also be moved when their condition within the organization changes to different groups and can even be removed entirely from all groups or access packages.

		• **Access reviews** help evaluate and validate access permissions and privileges granted to employees. • Identity governance solutions can also help enforce **Conditional Access policies**, like displaying a term of use and ensuring the user has agreed to those terms prior to accessing an application. • **Privileged Identity Management** provides additional controls tailored to securing access rights for resources, making sure users have just-in-time access to the right resources.
Data Integrity **(HIPAA Security Rule –** **§ 164.312(c)(1))**	• Only authorized users should have permission to modify PHI. IAM systems should restrict this based on user roles and responsibilities. • Any changes to PHI should be logged, tracked, and auditable through IAM tools.	• See Access Control and Audit Control sections above.
Physical and Logical Security **(HIPAA Security Rule –** **§ 164.310, § 164.312)**	• IAM systems should integrate with physical access control mechanisms, such as smartcards or biometric systems, to prevent unauthorized physical access to facilities where PHI is stored. • IAM should ensure that remote access to PHI is secure.	• Ensure only authorized individuals can access physical spaces by verifying their identity through a credential. Examples of physical credentials include badges, biometric scans (e.g., fingerprint, facial recognition), and YubiKeys.

Challenges and Best Practices

The challenges in implementing IAM for HIPAA Security Rule compliance include ensuring granular access control based on roles, managing multiple user identities and roles across dynamic healthcare environments, and establishing secure emergency access procedures. Organizations also struggle with timely provisioning and de-provisioning of user access, maintaining accurate audit trails and monitoring for suspicious activity, and effectively managing third-party vendor access while ensuring compliance with HIPAA's strict access and security requirements.

The following best practices are designed to address the challenges in managing an IAM system to ensure HIPAA compliance and protect PHI and ePHI from unauthorized access.

Best Practice	Description
Role-Based Access Control (RBAC)	Defining user roles and groups based on job responsibilities, granting access only to the minimum (least privilege access) PHI necessary for each role.
Multi-Factor Authentication (MFA)	An approach whereby a user's identity is validated to the trust level required according to a security policy for a resource being accessed using more than one factor (something you know (e.g., password), something you have (e.g., smartphone), something you are (e.g., fingerprint)
User Provisioning and De-provisioning	Automating the creation and termination of user accounts to ensure timely access provisioning and revocation, minimizing the risk of unauthorized access.
Emergency Access Procedures	Establishing secure emergency access mechanisms, with time-bound (JIT, PIM) and logged access, to ensure authorized personnel can access PHI in critical situations.
Continuous Monitoring and Audit Trails	Logging all access to PHI and monitoring it in real-time, generating audit trails for compliance audits, and detecting unauthorized access or anomalies.
Vendor and Third-Party Management	Implementing strict access controls for third-party vendors, ensuring they sign Business Associate agreements and have limited, monitored access.
Periodic Access Reviews	Regularly reviewing user access to ensure permissions are appropriate and aligning them with roles and the least privilege principle.
Data Encryption	Ensuring all PHI is encrypted both in transit and at rest, using strong encryption standards (e.g., AES-256 for storage, TLS 1.2+ for transmission).
Segregation of Duties (SoD)	Prevent conflicting roles by ensuring that one user cannot access PHI in ways that could lead to fraud, misuse, or errors by dividing responsibilities.
Compliance Audits and Reporting	Using automated tools for generating compliance reports, ensuring easy demonstration of adherence to HIPAA access and security requirements during audits.
Security Awareness Training	Providing ongoing training for all employees on HIPAA requirements, secure access practices, and recognizing phishing or social engineering attacks.

Future Trends in IAM and HIPAA

As the healthcare industry continues to evolve, tools and practices are also evolving to protect PHI and ePHI to ensure HIPPA compliance.

Trend	Description	Implications for IAM and HIPAA
Zero Trust Architecture (ZTA)	A ZTA security model assumes no implicit trust and continuously verifies	• Continuous identity verification and dynamic access controls. • Aligns with HIPAA's least privilege principle.

	access based on user behavior, device health, and context.	• Enhances real-time risk assessments.
AI and Machine Learning for IAM	AI and ML will enhance identity management and threat detection by analyzing user behavior, login patterns, and risk levels in real-time.	• Behavioral analytics for detecting suspicious access. • Automated risk assessments and predictive access controls. • Helps automate security audits for HIPAA compliance.
Biometric Authentication	Increased use of biometric authentication (fingerprint, facial recognition, etc.) as part of MFA for accessing PHI.	• Enhances security while providing a seamless user experience. • Meets HIPAA's strong authentication requirements. • Provides tamper-proof audit trails.
Cloud-Based IAM Solutions	The shift to cloud environments drives the adoption of cloud-based IAM solutions for managing identities and access across hybrid or multi-cloud environments.	• Scalable and centralized security management. • Ensures consistent enforcement of access policies across platforms. • Simplifies audit trail management for HIPAA compliance.
Blockchain for Access Control	Blockchain could provide tamper-proof audit trails and enable transparent access management to PHI with decentralized, immutable logs.	• Enhances audit trail security and accountability. • Blockchain smart contracts to enforce access policies. • Improves compliance with HIPAA's audit and accountability requirements.
Decentralized Identity (DID) Management	DID technologies will allow patients and healthcare providers to manage and verify access to PHI independently of central authorities.	• Empowers patients with control over their health data. • Ensures trusted identity verification. • Simplifies compliance with HIPAA's privacy and security rules.
Granular Consent Management and Patient-Centric IAM	IAM systems will provide more robust consent management tools, allowing patients to control who accesses their PHI and for what purposes.	• Improves patient rights and control over PHI. • Facilitates granular access controls for HIPAA compliance. • Enhances transparency in data access, ensuring accountability.
Enhanced Privacy Controls	IAM will incorporate advanced privacy controls and support regional/national privacy laws, helping healthcare organizations comply with data sovereignty requirements.	• Supports data sovereignty requirements and regional privacy laws. • Helps meet HIPAA Privacy Rule requirements. • Facilitates more efficient compliance audits.
Zero Knowledge Proof (ZPK)	IAM will incorporate ZPK, a method that allows a person to prove a claim without disclosing additional information. ZPK can be used to prove a user's identity without revealing their actual identity (e.g., username or	• Enhanced Security: ZPKs provide a mechanism for verifying authenticity without exposing underlying data, reducing the risk of data breaches or malicious attacks.

	password). This can secure the authentication process and prevent hackers from stealing the user's identity.	• Enables decentralized systems within healthcare (such as patient data management platforms or blockchain-based systems) to maintain privacy and security while still allowing for verifiable action
Post-Quantum Cryptography (PQC)	IAM platforms will integrate post-quantum cryptography to protect sensitive user authentication processes, such as passwords and biometric data, from quantum threats. These platforms will transition to quantum-resistant algorithms for secure identity verification, user access controls, and data protection. Note: PQC is being adopted as the FIPS standard. Future modifications to HIPAA will likely require adherence to PQC requirements	• Enhances the security of identity verification and access control. • Post-quantum methods will strengthen MFA mechanisms in identity platforms, preventing unauthorized access to healthcare systems while adhering to HIPAA's stringent access control policies.

Conclusion

IAM plays a crucial role in HIPAA compliance by ensuring the confidentiality, integrity, and availability of PHI and ePHI; it establishes the foundational security framework for controlling who can access what data and under what conditions, helping healthcare organizations meet several key HIPAA Security Rule requirements.

IAM ensures access to PHI and ePHI is managed, monitored, and logged, while ongoing security practices—such as risk assessments, training, encryption, and incident response—ensure that patient data remains protected in an increasingly complex healthcare environment. By implementing security protocols and a culture of continuous improvement, healthcare organizations can safeguard patient information and remain compliant with HIPAA's requirements.

Sources

[1] Office for Civil Rights. (2024, September 27). *The HIPAA Privacy Rule.* U.S. Department of Health and Human Services. https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

[2] Office for Civil Rights. (2022, October 20). *The Security Rule.* U.S. Department of Health and Human Services. https://www.hhs.gov/hipaa/for-professionals/security/index.html

[3] Office for Civil Rights. (2024, August 21). *Covered Entities and Business Associates.* U.S. Department of Health and Human Services. https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html

[4] The HIPAA Journal. (n.d.). *What are the Penalties for HIPAA Violations?* The HIPAA Journal. https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/

[5] Alder, S. (2024, January 12). *What did the HIPAA Omnibus Rule Mandate?* The HIPAA Journal. https://www.hipaajournal.com/hipaa-omnibus-rule/

[6] Alder, S. (2024, December 5). *What is the HITECH Act?* The HIPAA Journal. https://www.hipaajournal.com/what-is-the-hitech-act/

[7] Department of Health and Human Services, Office of the Secretary. (2025, January 6). *HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information.* Federal Register. https://www.federalregister.gov/documents/2025/01/06/2024-30983/hipaa-security-rule-to-strengthen-the-cybersecurity-of-electronic-protected-health-information

[8] Medical Group Management Association. (2025, February 17). *MGMA urges Trump Administration to rescind proposed HIPAA Security Rule.* Medical Group Management Association. https://www.mgma.com/advocacy-letters/february-17-2025-mgma-urges-trump-adminsitration-to-rescind-proposed-hipaa-security-rule

[9] National Institute of Standards and Technology. (n.d.). *Least Privilege.* NIST: Computer Security Resource Center. https://csrc.nist.gov/glossary/term/least_privilege

[10] Office for Civil Rights. (2024, July 19). *HIPAA Information Privacy for Professionals.* U.S. Department of Health and Human Services. https://www.hhs.gov/hipaa/for-professionals/index.html

[11] Marron, J.A. (2024, February). *NIST SP 800-66r2: Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide.* NIST: National Institute of Standards and Technology, U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-66r2.pdf

[12] Department of Health and Human Services. (2000). *§160.103.* GovInfo. https://www.govinfo.gov/content/pkg/CFR-2013-title45-vol1/pdf/CFR-2013-title45-vol1-sec160-103.pdf

[13] Flanagan, Heather. (2022). *Terminology in the IDPro Body of Knowledge.* ID Pro Body of Knowledge. https://bok.idpro.org/article/id/41/

[14] Office of the Federal Register. (n.d.). *A Guide to the Rulemaking Process.* Federal Register. https://www.federalregister.gov/uploads/2011/01/the_rulemaking_process.pdf

[15] Federal Trade Commission. (n.d.). *Understanding the NIST Cybersecurity Framework.* Federal Trade Commission. https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework#:~:text=NIST%20is%20the%20National%20Institute,The%20Framework%20is%20voluntary.

[16] Kibbe, D.C. (2001). *What the HIPAA Transactions and Code Set Standards Will Mean for Your Practice.* AFFP FPM. https://www.aafp.org/pubs/fpm/issues/2001/1100/p28.html#:~:text=The%20HIPAA%20transactions%20and%20code%20set%20standards%20are%20rules%20to,to%20computer%20without%20human%20involvement.

[17] Rose, S., Borchert O., Mitchell S., Connelly, S. (2020, August). *NIST Special Publication 800-207: Zero Trust Architecture.* National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

[18] Koot, A., (2020). *Introduction to Access Control (v4).* ID Pro Body of Knowledge. https://bok.idpro.org/article/id/42

[21] Office for Civil Rights. (2017, July 25). *HIPAA Enforcement.* U.S. Department of Health and Human Services. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html#:~:text=HIPAA%20Enforcement,on%20current%20or%20potential%20investigations.

Author Bios

Sharon Chahal is a Principal Product Manager in the Microsoft Security Customer Experiencing Engineering team for Identity and Network Access. Sharon leads a team of deep technical experts helping enterprise organizations deploy Entra ID within their environments. With 25+ years in the industry, she is a trusted advisor and is leading efforts in platform improvements to support healthcare regulatory compliance.

Hanita Epstein is a Senior Product Manager in the Microsoft Security Customer Experiencing Engineering team for Identity and Network Access. Prior to joining Microsoft, she was a data analytics consultant and a healthcare technology consultant.