Kiteworks

HIPAA Compliance in 2025: Navigating Enhanced Security Requirements and Rising Enforcement

Table of Contents

Executive Summary

The Health Insurance Portability and Accountability Act (HIPAA) stands as the cornerstone of healthcare information protection in the United States, establishing national standards that safeguard the privacy and security of protected health information (PHI) (U.S. Department of Health and Human Services, n.d.-b). Enacted in 1996 and continuously evolving through regulatory updates, HIPAA affects millions of healthcare organizations across diverse industries and geographic regions (U.S. Department of Health and Human Services, n.d.-b). The regulation encompasses three primary components—the Privacy Rule, Security Rule, and Breach Notification Rule—each addressing critical aspects of healthcare data protection (U.S. Department of Health and Human Services, n.d.-c).

U.S. Department of Health and Human Services

Organizations subject to HIPAA compliance include health plans, healthcare clearinghouses, healthcare providers conducting electronic transactions, and their business associates (U.S. Department of Health and Human Services, n.d.-d). The regulation's reach extends beyond traditional healthcare settings to encompass insurance companies, third-party administrators, technology vendors, billing services, and any entity handling PHI on behalf of covered entities (U.S. Department of Health and Human Services, n.d.-d).

Recent enforcement actions demonstrate the significant financial and reputational risks associated with noncompliance. In 2025 year to date, the Office for Civil Rights (OCR) has imposed fines and settlements totaling over $7.3 million (HIPAA Journal, 2025). These enforcement actions underscore the critical importance of maintaining robust compliance programs and the severe consequences of inadequate security measures.

Figure 1. 2025 HIPAA Violation Fines and Settlements[1]

Entity	Amount
BayCare Health System	$800,000
Comprehensive Neurology	$25,000
Comstar LLC	$75,000
Deer Oaks – The Behavioral Health Solution	$225,000
Guam Memorial Hospital Authority	$25,000
Health Fitness Corporation	$227,816
Northeast Radiology	$350,000
Oregon Health & Science University	$200,000
PIH Health	$600,000
Vision Upright MRI	$5,000
Warby Parker, Inc.	$1,500,000

[1] https://www.hipaajournal.com/hipaa-violation-fines/

Introduction

Healthcare organizations operate in an environment where sensitive personal information flows continuously between providers, payers, and service partners. This constant exchange of protected health information creates both opportunities for improved patient care and significant risks for data exposure. HIPAA provides the regulatory framework that balances these competing interests, establishing clear standards for protecting patient privacy while enabling the legitimate use and disclosure of health information necessary for treatment, payment, and healthcare operations (U.S. Department of Health and Human Services, n.d.-b).

The regulation's impact extends far beyond the healthcare sector itself. Technology companies developing healthcare applications, cloud service providers storing medical records, billing companies processing insurance claims, and legal firms handling healthcare matters must all understand and implement HIPAA compliance measures (U.S. Department of Health and Human Services, n.d.-d). This broad applicability reflects the interconnected nature of modern healthcare delivery and the need for consistent security standards across all participants in the healthcare ecosystem.

Figure 2. A Covered Entity is one of the following:[2]

A Health Care Provider

This includes providers such as:

- Doctors
- Clinics
- Psychologists
- Dentists
- Chiropractors
- Nursing Homes
- Pharmacies

... but only if they transmit any information in an electronic form in connection with a transaction for which HHS has adopted a standard.

A Health Plan

This includes:

- Health insurance companies
- HMOs
- Company health plans
- Government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans health care programs

A Health Care Clearinghouse

This includes entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.

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

The current regulatory landscape presents both challenges and opportunities for healthcare organizations. Recent cybersecurity threats, including ransomware attacks and data breaches, have prompted the OCR to strengthen enforcement efforts and propose significant updates to existing regulations. Organizations must now navigate not only established compliance requirements but also emerging regulatory initiatives designed to address evolving security threats. The December 2024 Notice of Proposed Rulemaking (NPRM) for the Security Rule represents the most significant update to HIPAA security requirements since the rule's inception, introducing new mandatory safeguards and eliminating the distinction between required and addressable implementation specifications (U.S. Department of Health and Human Services, 2024).

Understanding HIPAA compliance requires recognition of its three core components and their specific requirements. The Privacy Rule establishes standards for the use and disclosure of PHI (U.S. Department of Health and Human Services, n.d.-b). The Security Rule focuses on protecting electronic PHI through administrative, physical, and technical safeguards (U.S. Department of Health and Human Services, n.d.-c). The Breach Notification Rule requires organizations to notify patients, the media, and federal authorities when unsecured PHI is compromised (U.S. Department of Health and Human Services, n.d.-e). These rules work together to create a comprehensive framework for healthcare information protection.

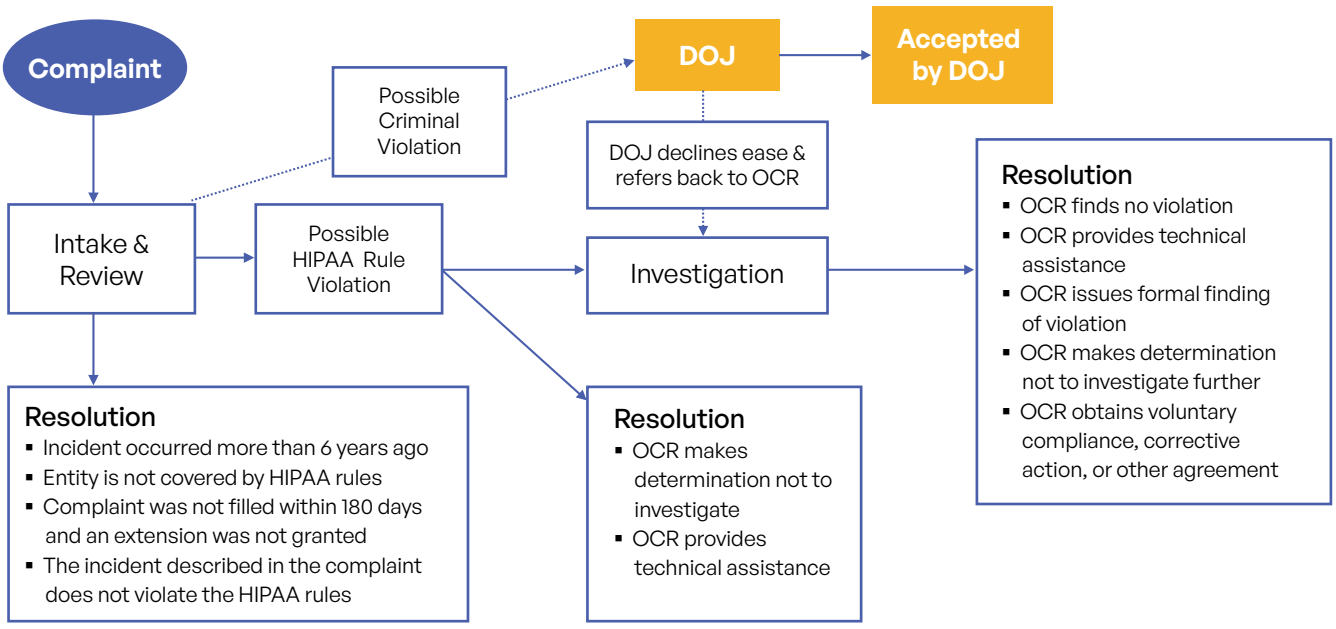
*The Privacy Rule establishes standards for the use and disclosure of PHI (U.S. Department of Health and Human Services, n.d.-b). The Security Rule focuses on **protecting electronic PHI through administrative, physical, and technical safeguards** (U.S. Department of Health and Human Services, n.d.-c). The Breach Notification Rule requires organizations to notify patients, the media, and federal authorities when unsecured PHI is compromised (U.S. Department of Health and Human Services, n.d.-e).*

The Privacy Rule: Protecting Patient Information Rights

The HIPAA Privacy Rule establishes the foundation for patient information protection by defining protected health information and establishing standards for its use and disclosure. This rule applies to all individually identifiable health information held or transmitted by covered entities and their business associates, regardless of format—electronic, paper, or oral (U.S. Department of Health and Human Services, n.d.-b). The rule's comprehensive scope ensures consistent protection standards across all forms of health information, recognizing that patient privacy concerns extend beyond electronic systems to encompass all methods of information handling.

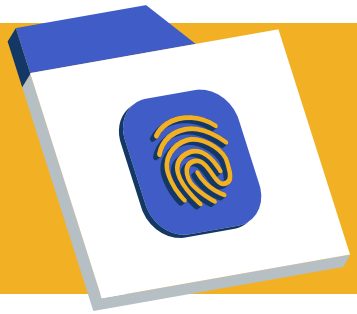
Covered entities under the Privacy Rule include health plans, healthcare clearinghouses, and healthcare providers who transmit health information electronically in connection with standard transactions (U.S. Department of Health and Human Services, n.d.-d). A "business associate" under HIPAA is any person or entity that performs functions or activities involving the use or disclosure of protected health information on behalf of a covered entity (like a healthcare provider or health plan), excluding the covered entity's own workforce members. Examples include third-party administrators processing claims, CPAs with access to patient data during accounting services, consultants performing utilization reviews, medical transcriptionists, and pharmacy benefits managers—essentially any external party handling protected health information while providing services like billing, data analysis, legal work, or administrative support to covered entities. Health plans encompass individual and group insurance plans, health maintenance organizations, Medicare, Medicaid, and employer-sponsored group health plans. Healthcare clearinghouses process nonstandard health information into standard formats or vice versa, including billing services and community health management information systems. Healthcare providers include hospitals, physicians, dentists, and other practitioners who electronically transmit health information for standard transactions such as claims processing or benefit eligibility inquiries.

Figure 3. HIPAA Complaint Process[3]



[3]https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/enforcement-process/index.html

The Privacy Rule establishes the fundamental principle that covered entities may not use or disclose protected health information except as specifically permitted or required by the rule or as authorized by the individual (U.S. Department of Health and Human Services, n.d.-b). This principle creates a presumption against disclosure, placing the burden on covered entities to justify any use or sharing of patient information. The rule permits certain uses and disclosures without individual authorization, including treatment, payment, and healthcare operations activities, as well as specific public interest purposes such as public health activities, law enforcement, and research conducted under specific conditions (U.S. Department of Health and Human Services, n.d.-b).



*The Privacy Rule establishes the fundamental principle that covered entities may **not use or disclose protected health information except as specifically permitted or required by the rule or as authorized by the individual** (U.S. Department of Health and Human Services, n.d.-b).*

Individual rights under the Privacy Rule empower patients to access their medical records, request amendments, restrict disclosures, and receive an accounting of disclosures (U.S. Department of Health and Human Services, n.d.-b). Patients have the right to access their medical records, request amendments to inaccurate information, request restrictions on uses and disclosures, and receive an accounting of disclosures made by their healthcare providers. These rights empower patients to participate actively in protecting their privacy and ensure transparency in how their information is handled. Healthcare organizations must establish procedures to accommodate these rights and respond to patient requests within specified timeframes.

The minimum necessary standard further requires reasonable efforts to limit PHI disclosure to the minimum necessary to accomplish the intended purpose, with exceptions for treatment activities and individual requests (U.S. Department of Health and Human Services, n.d.-b). This standard applies to most uses and disclosures but includes important exceptions for treatment activities, disclosures to the individual, and uses or disclosures made pursuant to individual authorization. Organizations must develop and implement policies and procedures that restrict access to protected health information based on workforce members' roles and responsibilities.

Business associate relationships are governed by contracts mandating Privacy Rule safeguards and breach reporting obligations (U.S. Department of Health and Human Services, n.d.-d). The HITECH Act expanded direct liability to business associates, enabling OCR to enforce penalties against them (U.S. Department of Health and Human Services, 2009). When covered entities engage contractors or other parties to perform functions involving protected health information, they must execute business associate agreements that impose specified safeguards on the information. These agreements must require business associates to protect the information consistent with the Privacy Rule and to report any security incidents or breaches. The expansion of business associate liability under the HITECH Act means that business associates face direct enforcement action for Privacy Rule violations.

Privacy practices notices serve as the primary mechanism for informing patients about how their health information may be used and disclosed. Covered entities must also provide privacy practices notices to patients at first service encounter, describing organizational privacy practices and patient rights (U.S. Department of Health and Human Services, n.d.-b). The notices must describe the organization's privacy practices, patient rights, and contact information for filing complaints. Healthcare providers must make good faith efforts to obtain written acknowledgment of notice receipt, though failure to obtain acknowledgment does not prevent treatment.

Enforcement of the Privacy Rule includes civil monetary penalties—up to $1.9 million per violation category per year—and criminal penalties ranging from $50,000 and one year imprisonment to $250,000 and ten years imprisonment for knowing violations (U.S. Department of Health and Human Services, n.d.-b).

The Security Rule: Safeguarding Electronic Health Information

The HIPAA Security Rule establishes national standards for protecting electronic PHI (ePHI) through administrative, physical, and technical safeguards (U.S. Department of Health and Human Services, n.d.-c). It applies to the same covered entities as the Privacy Rule, as well as their business associates (U.S. Department of Health and Human Services, n.d.-c). The rule's flexible, scalable approach allows organizations of different sizes and types to implement appropriate security measures while meeting consistent baseline requirements.

*The HIPAA Security Rule establishes national standards for **protecting electronic PHI (ePHI) through administrative, physical, and technical safeguards** (U.S. Department of Health and Human Services, n.d.-c).*

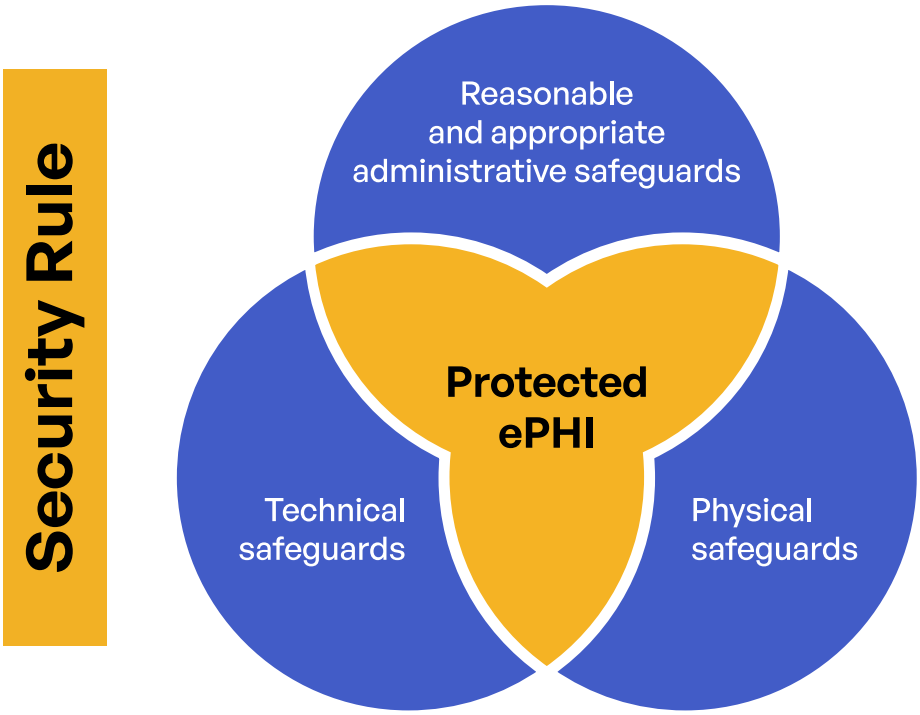
The Security Rule applies to the same covered entities as the Privacy Rule—health plans, healthcare clearinghouses, and healthcare providers who transmit health information electronically—as well as their business associates. The HITECH Act extended direct liability to business associates, meaning these organizations face the same enforcement risks as covered entities when they fail to implement required security safeguards. This expansion recognizes the critical role that business associates play in the healthcare ecosystem and the need for consistent security standards across all entities handling electronic protected health information.

Electronic protected health information encompasses any protected health information maintained or transmitted in electronic form. This includes information stored in electronic health records, transmitted via email or other electronic communication methods, and maintained on portable devices such as laptops or smartphones. The rule's broad definition ensures comprehensive protection for electronic health information regardless of the specific technology used to store or transmit it.

Administrative safeguards require policies and procedures such as risk analysis, workforce training, information access management, and incident response planning (U.S. Department of Health and Human Services, n.d.-c). These safeguards include security management processes, assigned security responsibilities, workforce training, information access management, and security incident procedures. Organizations must designate a security official responsible for developing and implementing security policies and procedures, conduct regular security awareness training for all workforce members, and establish procedures for responding to security incidents.

The risk analysis requirement compels organizations to assess potential risks and vulnerabilities to ePHI, forming the basis for reasonable and appropriate security measures (U.S. Department of Health and Human Services, n.d.-c). This analysis must consider the organization's size, complexity, and capabilities, as well as its technical infrastructure and the costs of security measures. The risk analysis serves as the foundation for determining which security measures are reasonable and appropriate for the organization's specific circumstances.

Physical safeguards protect electronic information systems and related workstations from physical threats and environmental hazards. These requirements include facility access controls, workstation use restrictions, and device and media controls (U.S. Department of Health and Human Services, n.d.-c). Organizations must implement policies and procedures to limit physical access to electronic information systems while ensuring that authorized personnel can access systems as needed. Workstation use requirements specify proper use of workstations that access electronic protected health information, including restrictions on workstation location and user access.



Technical safeguards use technology to protect electronic protected health information and control access to it. These requirements include access control, audit controls, integrity controls, person or entity authentication, and transmission security (U.S. Department of Health and Human Services, n.d.-c). Access control measures ensure that only authorized persons can access electronic protected health information, while audit controls create records of information system activity. Integrity controls protect electronic protected health information from improper alteration or destruction, and authentication procedures verify the identity of persons seeking access to electronic protected health information.

The Security Rule's flexibility allows organizations to implement security measures appropriate to their specific circumstances while meeting the rule's requirements. This approach recognizes that a small physician practice has different security needs and resources than a large hospital system. However, recent enforcement actions and the proposed Security Rule updates indicate that regulators expect organizations of all sizes to implement robust security measures consistent with current cybersecurity best practices.

At this time, implementation specifications within the Security Rule are categorized as either required or addressable. Required specifications must be implemented by all covered entities and business associates. Addressable specifications allow organizations to determine whether the specification is reasonable and appropriate for their situation. If an addressable specification is not reasonable and appropriate, the organization must implement an alternative measure that accomplishes the same purpose or document why implementing the specification or an alternative measure is not reasonable and appropriate (U.S. Department of Health and Human Services, n.d.-c).

The December 2024 Notice of Proposed Rulemaking represents the most significant update to the Security Rule since its inception, proposing to eliminate the distinction between required and addressable implementation specifications and making all specifications required with limited exceptions (U.S. Department of Health and Human Services, 2024). This change reflects the evolving cybersecurity threat landscape and the need for more robust security standards across all healthcare organizations.

The Breach Notification Rule: Responding to Security Incidents

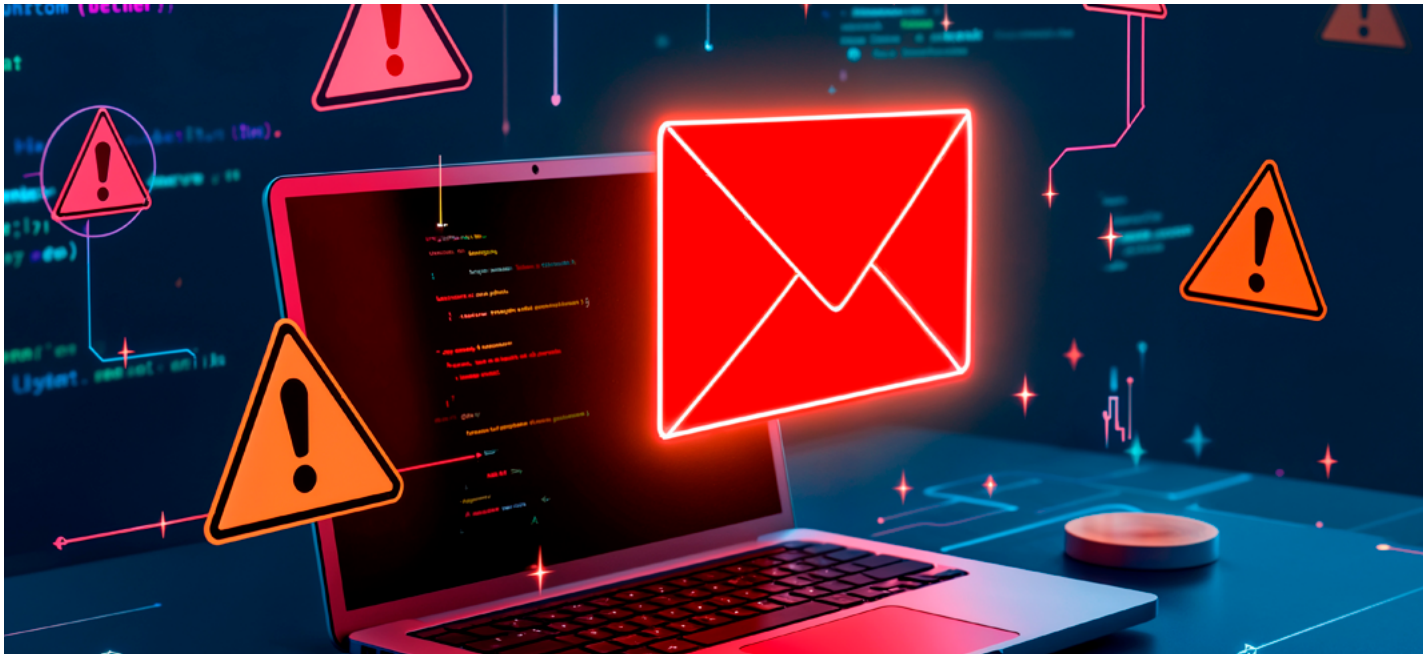
The HIPAA Breach Notification Rule establishes requirements for notifying patients, the media, and federal authorities when unsecured protected health information is compromised (U.S. Department of Health and Human Services, n.d.-e). A breach is defined as the unauthorized acquisition, access, use, or disclosure of PHI that compromises its security or privacy (U.S. Department of Health and Human Services, n.d.-e). This rule recognizes that despite best efforts to protect health information, breaches can occur, and affected individuals have the right to know when their information has been compromised. The rule's notification requirements serve multiple purposes: protecting individuals from potential harm,

maintaining public trust in the healthcare system, and providing regulators with information necessary to identify systemic security problems. The breach notification requirements apply to covered entities and business associates when they discover breaches of unsecured protected health information. A breach is defined as the acquisition, access, use, or disclosure of protected health information in a manner not permitted by the Privacy Rule that compromises the security or privacy of the information.

*The **HIPAA Breach Notification Rule** establishes requirements for notifying patients, the media, and federal authorities when unsecured protected health information is compromised.*

Unsecured protected health information refers to information that is not secured through the use of technology or methodology specified by the Secretary of Health and Human Services. The guidance specifies that information is secured if it is encrypted or destroyed according to specific standards. This definition incentivizes organizations to implement strong encryption and data destruction practices, as secured information is not subject to breach notification requirements even if it is improperly accessed or disclosed.

Breach notification requirements vary based on the number of individuals affected by the breach. For breaches affecting 500 or more individuals, covered entities must notify affected individuals without unreasonable delay but no later than 60 days after discovery of the breach. They must also notify the media serving the affected area and the Secretary of Health and Human Services contemporaneously with individual notification. For breaches affecting fewer than 500 individuals, covered entities must notify affected individuals within 60 days but can delay notification to the Secretary until the end of the calendar year (U.S. Department of Health and Human Services, n.d.-e).



Individual notification must include specific information about the breach, including a description of what happened, the types of information involved, steps individuals can take to protect themselves, and what the covered entity is doing to investigate and address the breach. The notification must be provided in writing by first-class mail or email if the individual has agreed to electronic notice. If contact information is insufficient or out of date, covered entities must provide substitute notice through prominent posting on their website or major media outlets.

Media notification requirements apply to breaches affecting 500 or more residents of a state or jurisdiction. Covered entities must notify prominent media outlets serving the affected area without unreasonable delay but no later than 60 days after discovery of the breach. This requirement ensures that large breaches receive public attention and helps individuals who may not have received direct notification become aware of the breach.

Figure 4. Cases Currently Under Investigation[4]

Name of Covered Entity	State	Covered Entity Type	Type of Breach	Individuals Affected
Anne Arundel Dermatology	MD	Healthcare Provider	Hacking/IT Incident	1,905,000
Ascension Health Services LLC dba Alpha Wellness & Alpha Medical Centre	GA	Healthcare Provider	Hacking/IT Incident	1,714
Cierant Corporation	CT	Business Associate	Hacking/IT Incident	232,506
Complete Care Rehab LLC	MI	Healthcare Provider	Hacking/IT Incident	4,764
Kotel ATX PLLC dba Heading Health	TX	Healthcare Provider	Unauthorized Access/ Disclosure	650
Naper Grove Vision Care	IL	Healthcare Provider	Hacking/IT Incident	501
Radiology Associates of Richmond, Inc.	VA	Healthcare Provider	Hacking/IT Incident	1,419,091
Regional Center of the East Bay	CA	Healthcare Provider	Unauthorized Access/ Disclosure	689
Urology Associates of Charleston	SC	Healthcare Provider	Hacking/IT Incident	2,060
Zumpano Patricios, P.A.	FL	Business Associate	Hacking/IT Incident	279,275

Business associates have specific notification obligations when they discover breaches of unsecured protected health information. They must notify the covered entity of the breach without unreasonable delay but no later than 60 days after discovery. The notification must include identification of each individual whose information was involved in the breach to the extent possible. This requirement ensures that covered entities receive timely information about breaches involving their patients' information and can fulfill their own notification obligations.

The Secretary of Health and Human Services maintains a public database of breaches affecting 500 or more individuals (U.S. Department of Health and Human Services, n.d.-a). This database provides transparency about large breaches and helps identify trends in healthcare data security incidents. Organizations listed in the database often experience significant reputational damage in addition to regulatory penalties, emphasizing the importance of preventing breaches through robust security measures.

[4] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Recent breach data reveals the growing scale and impact of healthcare cybersecurity incidents. In 2023, over 167 million individuals were affected by large breaches reported to OCR, representing a new record (U.S. Department of Health and Human Services, n.d.-a). The increase in breach size and frequency reflects the healthcare sector's growing reliance on electronic systems and the increasing sophistication of cyber threats targeting healthcare organizations. These trends underscore the critical importance of implementing comprehensive security measures and maintaining effective incident response capabilities.

*In 2023, over **167 million individuals** were affected by large breaches reported to OCR, representing a new record.*

Regulatory Initiatives: Evolving Standards and Requirements

The healthcare cybersecurity landscape continues to evolve quickly, driven by increasing threats, technological advances, and regulatory responses to emerging risks. Recent regulatory initiatives reflect federal authorities' recognition that existing HIPAA requirements, while foundational, require strengthening to address current cybersecurity challenges. The Office for Civil Rights has taken steps to update security standards and increase enforcement activities, signaling a new era of heightened regulatory scrutiny for healthcare organizations.

The December 2024 Notice of Proposed Rulemaking for the HIPAA Security Rule represents the most significant regulatory development since the rule's initial implementation. This proposed rule responds to alarming trends in healthcare cybersecurity incidents, including a 102% increase in large breach reports between 2018 and 2023 and a 1,002% increase in the number of individuals affected by such breaches (U.S. Department of Health and Human Services, 2024). The proposed changes acknowledge that current security standards, developed over two decades ago, no longer adequately address the sophisticated threats facing healthcare organizations today.

*The proposed changes acknowledge that current security standards, developed over two decades ago, **no longer adequately address** the sophisticated threats facing healthcare organizations today.*

The proposed rule introduces fundamental changes to Security Rule implementation requirements. Most significantly, it eliminates the distinction between required and addressable implementation specifications, making all specifications required with limited exceptions. This change reflects the reality that basic cybersecurity measures once considered optional are now essential for protecting against modern threats. The proposal recognizes that the healthcare sector's critical infrastructure status demands consistent, robust security standards across all organizations handling electronic protected health information.

Key provisions of the proposed rule include mandatory encryption of electronic protected health information at rest and in transit, multi-factor authentication requirements, network segmentation mandates, and regular vulnerability assessments. These requirements align with current cybersecurity best practices and reflect standards already implemented by many healthcare organizations. The proposed rule also introduces specific timelines for compliance activities, including 24-hour notification requirements for certain security incidents and annual compliance audits.

The proposed rule strengthens requirements for risk analysis and management, recognizing these activities as fundamental to effective cybersecurity programs. Organizations would be required to develop and maintain technology asset inventories and network maps, conduct more detailed risk assessments, and implement specific security controls based on their risk profiles. Contingency planning and incident response requirements receive significant attention in the proposed rule, reflecting the critical importance of organizational resilience in the face of cyber threats. Organizations would be required to establish procedures for restoring critical systems within 72 hours, develop comprehensive security incident response plans, and conduct regular testing of these plans.

The proposed rule also addresses business associate oversight and accountability, requiring enhanced verification procedures and reporting requirements. Business associates would be required to provide annual certifications of their security compliance and notify covered entities within 24 hours of contingency plan activations.

Recent court decisions have also shaped the regulatory landscape, particularly regarding privacy protections for reproductive health information. In June 2025, a federal court in Texas vacated most of the HIPAA Privacy Rule modifications related to reproductive health care privacy, while leaving other privacy practice notice requirements intact. This decision highlights the ongoing legal challenges surrounding healthcare privacy regulations and the need for organizations to stay current with evolving requirements.

The Biden administration's National Cybersecurity Strategy has influenced healthcare cybersecurity policy, emphasizing the need for stronger security standards and greater accountability for critical infrastructure sectors. The Department of Health and Human Services has aligned its regulatory initiatives with this broader cybersecurity strategy, positioning the proposed Security Rule updates as part of a comprehensive approach to protecting critical infrastructure.

Violations and Enforcement: Understanding Compliance Risks

HIPAA enforcement activities have intensified significantly in recent years, with the Office for Civil Rights demonstrating increased willingness to pursue both civil monetary penalties and settlement agreements for violations (HIPAA Journal, 2025). The enforcement data from 2025 year to date reveals clear patterns in violation types, penalty amounts, and regulatory priorities that provide valuable insights for organizations developing compliance strategies. Understanding these trends helps organizations identify high-risk areas and allocate resources effectively to prevent violations.

Risk analysis failures represent the most common violation type in recent enforcement actions, appearing in nearly every settlement and penalty assessed 2025 year to date (HIPAA Journal, 2025). This pattern reflects the fundamental importance of risk analysis as the foundation of effective security programs and OCR's focus on ensuring organizations understand their security vulnerabilities. The prevalence of risk analysis violations demonstrates that many organizations continue to struggle with implementing comprehensive risk assessment processes despite clear regulatory requirements.

The financial impact of HIPAA violations has reached unprecedented levels, with total penalties and settlements exceeding $7.3 million 2025 year to date. Individual penalties range from $5,000 for small organizations to $1.5 million for large healthcare systems, reflecting the OCR's approach of scaling penalties based on organization size, violation severity, and culpability (HIPAA Journal, 2025). The largest settlement, imposed on Solara Medical Supplies, demonstrates the severe financial consequences of comprehensive security failures that result in large-scale data breaches.

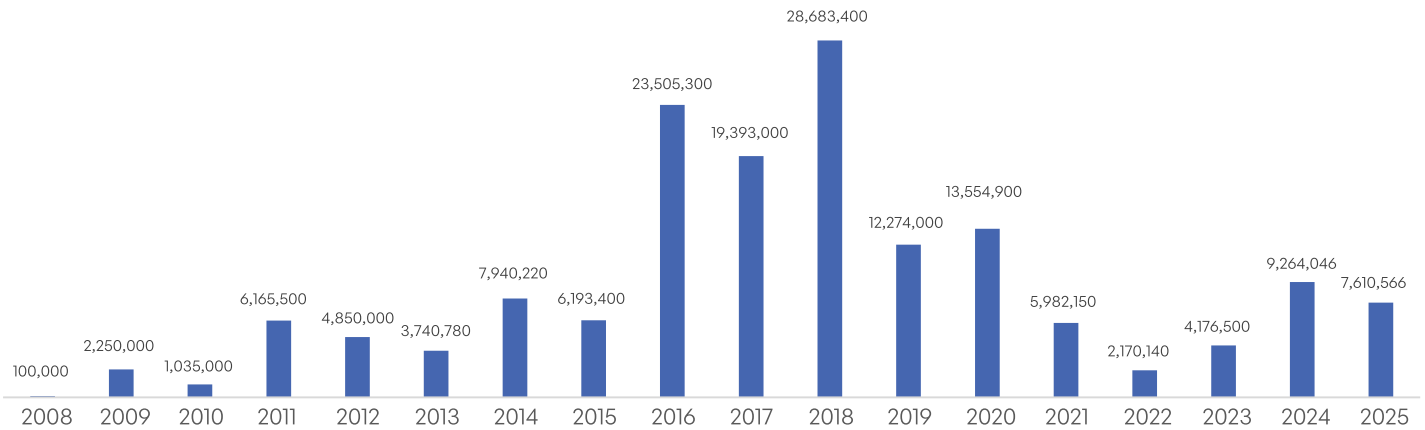
Warby Parker's $1.5 million civil monetary penalty represents a significant enforcement action against a business associate, highlighting OCR's commitment to holding all regulated entities accountable for Security Rule violations. This penalty, imposed for failures in risk analysis, risk management, and monitoring activities, demonstrates that business associates face the same enforcement risks as covered entities. The action serves as a clear warning to technology companies and other business associates that HIPAA compliance is not optional regardless of their primary business focus.

Settlement agreements typically include requirements for comprehensive corrective action plans, independent compliance monitoring, and regular reporting to OCR. These agreements often require organizations to implement specific security measures, conduct employee training, and engage third-party assessors to verify compliance. The corrective action requirements provide insights into OCR's expectations for comprehensive compliance programs and the specific measures organizations should implement to prevent violations.

Figure 5. 2025 HIPAA Violation Fines and Settlements[5]

Entity	Amount	Reason
BayCare Health System	$800,000	Information access management (minimum necessary standard), risk management, information system activity review
Comprehensive Neurology	$25,000	HIPAA Risk Analysis violation
Comstar LLC	$75,000	Risk analysis failure
Deer Oaks – The Behavioral Health Solution	$225,000	Risk analysis failure; impermissible disclosure of ePHI
Guam Memorial Hospital Authority	$25,000	HIPAA Risk Analysis violation
Health Fitness Corporation	$227,816	HIPAA Risk Analysis violation
Northeast Radiology	$350,000	HIPAA Risk Analysis violation
Oregon Health & Science University	$200,000	Violation of the HIPAA Right of Access
PIH Health	$600,000	HIPAA Risk Analysis violation, impermissible disclosure of the ePHI of 189,763 individuals, failure to issue a media breach notice, failure to issue timely breach notifications to the HHS, and the affected patients
Syracuse ASC, dba Specialty Surgery Center of Central New York	$250,000	Risk analysis failure; untimely data breach notifications to the HHS Secretary & individuals
Vision Upright MRI	$5,000	HIPAA Risk Analysis violation, HIPAA breach notification violation
Warby Parker, Inc.	$1,500,000	Violation of the HIPAA Security Rule: Risk analysis, risk management, and monitoring activity in information systems containing ePHI

Figure 6. Total HIPAA Settlements and Civil Monetary Penalties (2008-2025)[6]



[5,6]https://www.hipaajournal.com/hipaa-violation-fines/

The enforcement trends reveal OCR's strategic approach to maximizing compliance impact through targeted enforcement actions. By focusing on fundamental requirements such as risk analysis and publicizing enforcement actions, OCR creates incentives for voluntary compliance across the healthcare industry. The agency's enforcement strategy appears designed to send clear messages about compliance expectations while providing organizations with practical guidance on addressing common violation areas.

Recent enforcement actions also demonstrate OCR's increased focus on business associate compliance, reflecting the expanded role these organizations play in the healthcare ecosystem. As healthcare organizations increasingly rely on third-party vendors for technology services, data processing, and administrative functions, ensuring business associate compliance becomes critical for overall security and privacy protection. The enforcement actions against business associates signal that these organizations can no longer rely on covered entities to bear primary responsibility for compliance.

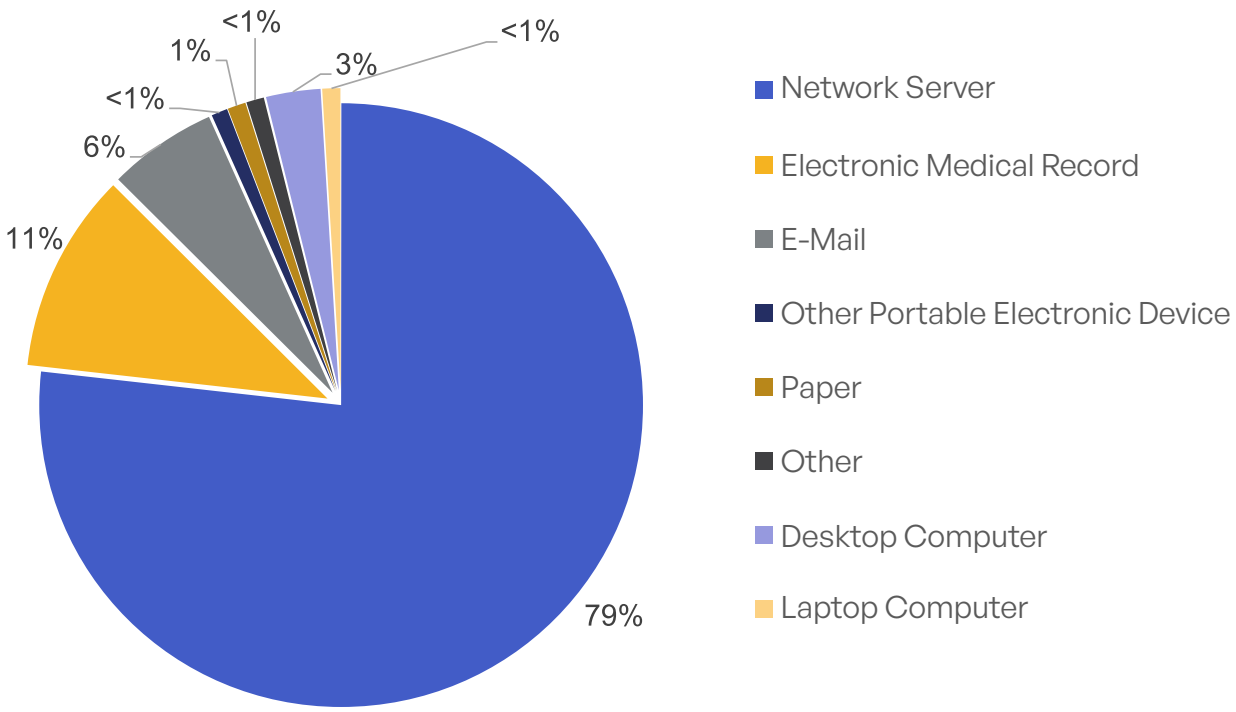
Looking forward, the proposed Security Rule updates suggest that enforcement activity will continue to intensify as new requirements take effect. Organizations that proactively address current compliance gaps and prepare for proposed rule changes will be better positioned to avoid enforcement actions and demonstrate good faith compliance efforts. The enforcement trends provide clear guidance on regulatory priorities and the specific areas where organizations should focus their compliance efforts.

Compliance Expectations and Related Regulations

Organizations subject to HIPAA face comprehensive compliance expectations that extend beyond mere technical security measures to encompass organizational culture, governance structures, and operational processes. The regulation demands a holistic approach to privacy and security that integrates legal requirements with business operations and clinical workflows. Understanding these expectations helps organizations develop effective compliance programs that address both regulatory requirements and practical operational needs.

The fundamental compliance expectation under HIPAA is the establishment of administrative, physical, and technical safeguards that protect the confidentiality, integrity, and availability of protected health information. This expectation requires organizations to implement comprehensive security programs that address all aspects of information handling, from initial collection through final disposal. The safeguards must be reasonable and appropriate for the organization's specific circumstances while meeting minimum baseline requirements established by the regulations.

Figure 7. HHS Office for Civil Rights Breaches of Unsecured PHI Affecting 500 or More Individuals in 2022 by Percentage of Individuals Affected by Location of PHI[7]



Risk management serves as the foundation of HIPAA compliance, requiring organizations to conduct thorough assessments of potential threats and vulnerabilities to protected health information. This expectation goes beyond simple checklists to demand sophisticated analysis of organizational risks, threat landscapes, and vulnerability management. Organizations must demonstrate that their security measures are based on comprehensive risk assessments and that they regularly update these assessments to address changing circumstances.

Documentation requirements under HIPAA create significant compliance expectations for maintaining comprehensive records of policies, procedures, training activities, and security measures. Organizations must document not only their compliance efforts but also their decision-making processes, risk assessments, and incident response activities. This documentation serves multiple purposes: demonstrating compliance during regulatory investigations, supporting internal compliance monitoring, and providing evidence of good faith compliance efforts.

[7]https://www.hhs.gov/sites/default/files/breach-report-to-congress-2022.pdf

Workforce training and management expectations require organizations to ensure that all employees understand their responsibilities for protecting health information and are equipped with the knowledge and tools necessary to comply with HIPAA requirements. This expectation extends beyond one-time training to encompass ongoing education, role-specific training, and regular competency assessments. Organizations must also implement appropriate sanctions for employees who violate privacy and security policies.

Business associate management represents a critical compliance expectation that requires organizations to carefully evaluate and monitor third-party relationships involving protected health information. Organizations must conduct due diligence on potential business associates, negotiate appropriate contractual protections, and monitor ongoing compliance with contractual obligations. This expectation recognizes that healthcare organizations' security depends not only on their own measures but also on the security practices of their business partners.

Figure 8. 12 Important Elements of HIPAA Training[8]

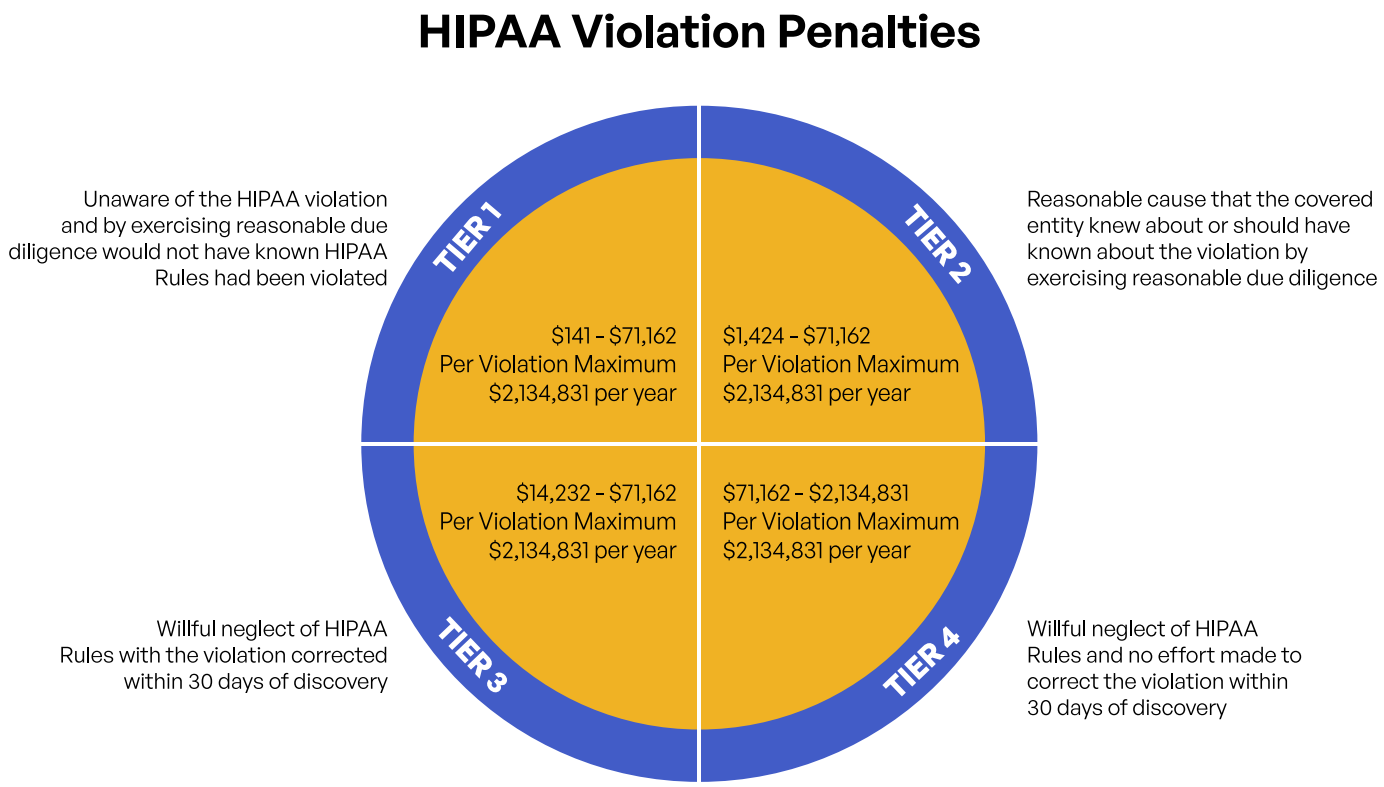
*Organizations must **conduct due diligence** on potential business associates, negotiate appropriate contractual protections, and monitor ongoing compliance with **contractual obligations**.*

[8]https://www.hipaajournal.com/hipaa-training-requirements/

Incident response capabilities represent essential compliance expectations that require organizations to detect, investigate, and respond to security incidents involving protected health information. Organizations must establish formal incident response procedures, maintain incident response teams, and conduct regular testing of their response capabilities. The expectation extends to breach notification requirements and coordination with law enforcement and regulatory authorities when appropriate.

Related regulations create additional compliance obligations for healthcare organizations beyond HIPAA requirements. The HITECH Act strengthened HIPAA's enforcement mechanisms and extended liability to business associates, while also establishing additional privacy protections for genetic information. State privacy laws may impose additional requirements or provide greater protections than HIPAA, requiring organizations to comply with the most stringent applicable standards.

Figure 9. Penalty Structure for HIPAA Violations[9]



The FDA's cybersecurity guidance for medical devices creates additional compliance expectations for healthcare organizations that use networked medical devices. Organizations must consider medical device cybersecurity risks as part of their overall security programs and coordinate with device manufacturers to address vulnerabilities and security updates. This requirement reflects the growing connectivity of medical devices and the associated cybersecurity risks.

Financial regulations may also apply to healthcare organizations, particularly those that handle payment card information or provide financial services. The Payment Card Industry Data Security Standard (PCI DSS) creates additional security requirements for organizations that process credit card payments, while banking regulations may apply to healthcare organizations that provide financial services or maintain patient financial information.

[9]https://www.hipaajournal.com/hipaa-violation-fines/

Federal Trade Commission regulations regarding unfair or deceptive practices may apply to healthcare organizations' privacy and security practices, particularly in cases where organizations fail to implement promised security measures or misrepresent their privacy practices. The FTC's enforcement authority provides an additional layer of regulatory oversight for healthcare organizations' privacy and security practices.

State breach notification laws may impose additional requirements beyond HIPAA's breach notification rule, requiring organizations to notify state authorities or provide additional information to affected individuals. Organizations must understand both federal and state breach notification requirements to ensure comprehensive compliance with all applicable notification obligations.

Figure 10. Notification to the Secretary[10]

> (b) *Implementation specifications: Breaches involving 500 or more individuals.* For breaches of unsecured protected health information involving 500 or more individuals, a covered entity shall, except as provided in §164.412, provide the notification required by paragraph (a) of this section contemporaneously with the notice required by §164.404(a) and in the manner specified on the HHS Web site.
>
> (c) *Implementation specifications: Breaches involving less than 500 individuals.* For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required by paragraph (a) of this section for breaches discovered during the preceding calendar year, in the manner specified on the HHS web site.

The proposed Security Rule updates will significantly expand compliance expectations by requiring specific security measures that are currently optional or recommended. Organizations must prepare for these enhanced requirements by assessing their current security posture, identifying gaps with proposed requirements, and developing implementation plans for new security measures. The proposed rule's emphasis on encryption, multi-factor authentication, and network segmentation reflects evolving cybersecurity best practices and regulatory expectations.

[10]https://www.govinfo.gov/content/pkg/CFR-2018-title45-vol1/pdf/CFR-2018-title45-vol1-sec164-408.pdf

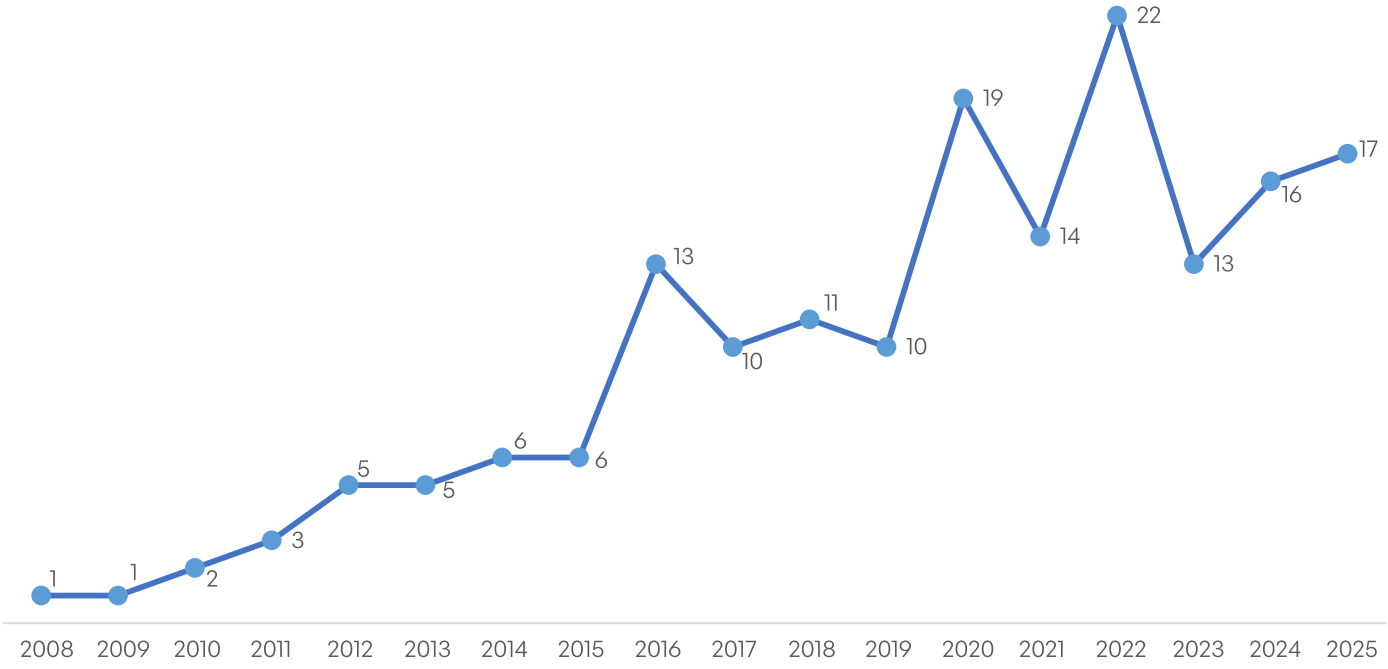
The Current State of HIPAA Enforcement

The Office for Civil Rights has demonstrated increased enforcement activity in recent years, reflecting both the agency's increased resources and its strategic focus on healthcare cybersecurity. The enforcement landscape has evolved from primarily complaint-driven investigations to include proactive compliance reviews, targeted enforcement initiatives, and comprehensive settlement agreements that address systemic compliance failures. This evolution represents a fundamental shift in regulatory approach that requires organizations to maintain continuous compliance rather than reactive remediation.

*The enforcement landscape has evolved from primarily **complaint-driven investigations to include proactive compliance reviews**, targeted enforcement initiatives, and comprehensive settlement agreements that address systemic compliance failures.*

Enforcement statistics reveal the scope and impact of OCR's increased activity. The agency has collected over $130 million in civil monetary penalties and settlements since 2003, with the majority of these penalties imposed in recent years. The escalating penalty amounts reflect both the increasing severity of violations and OCR's willingness to impose substantial financial consequences for noncompliance. The trend toward larger penalties demonstrates that healthcare organizations can no longer treat HIPAA compliance as a minimal regulatory requirement.

Figure 11. OCR Penalties for HIPAA Violations (2008 - 2025)[11]



[11]https://www.hipaajournal.com/hipaa-violation-fines/

The enforcement data reveals clear patterns in violation types and penalty assessments. Risk analysis failures appear in nearly every enforcement action in 2025, highlighting this requirement's fundamental importance and the widespread compliance failures in this area. The consistency of risk analysis violations across different organization types and sizes indicates that many healthcare organizations continue to struggle with implementing comprehensive risk assessment processes despite clear regulatory guidance. Settlement agreements have become the OCR's preferred enforcement mechanism, allowing the agency to achieve comprehensive compliance improvements while avoiding lengthy litigation processes. These agreements typically require organizations to implement specific corrective actions, engage independent compliance monitors, and submit regular compliance reports. The settlement approach enables OCR to address systemic compliance failures while providing organizations with clear guidance on regulatory expectations.

Civil monetary penalties have reached unprecedented levels, with individual penalties exceeding $1.5 million in recent cases. The penalty structure considers factors such as organization size, violation severity, and culpability, with the largest penalties reserved for organizations that demonstrate willful neglect or repeated violations. Criminal enforcement remains relatively rare but continues to serve as a deterrent for the most serious violations. The Department of Justice has prosecuted individuals for knowingly obtaining or disclosing protected health information, with penalties including substantial fines and imprisonment. These criminal cases typically involve intentional wrongdoing rather than compliance failures, but they demonstrate the serious legal consequences of HIPAA violations.

The proposed Security Rule updates will likely intensify enforcement activity as organizations struggle to implement new requirements. OCR has indicated that it will provide implementation guidance and technical assistance to help organizations comply with enhanced requirements. However, the agency has also made clear that it will hold organizations accountable for implementing required security measures within specified timeframes.

*The proposed Security Rule updates will likely **intensify enforcement activity** as organizations struggle to implement new requirements.*

Enforcement trends suggest that OCR will continue to focus on fundamental compliance requirements such as risk analysis, security incident procedures, and business associate management. Organizations that address these core requirements proactively will be better positioned to avoid enforcement actions and demonstrate good faith compliance efforts. The enforcement patterns provide clear guidance on regulatory priorities and the specific areas where organizations should focus their compliance efforts.

The enforcement landscape also reflects OCR's strategic approach to maximizing compliance impact through targeted enforcement actions. By focusing on common violation types and publicizing enforcement actions, OCR creates incentives for voluntary compliance across the healthcare industry. The agency's enforcement strategy appears designed to send clear messages about compliance expectations while providing organizations with practical guidance on addressing common violation areas.

Looking forward, organizations should expect continued enforcement activity as OCR maintains its focus on healthcare cybersecurity. The agency's increased resources and expanded enforcement authority provide the capability to pursue more enforcement actions while maintaining comprehensive settlement agreements. Organizations that invest in comprehensive compliance programs and proactive risk management will be better positioned to avoid enforcement actions and demonstrate their commitment to protecting patient information.

Five Essential Steps to HIPAA Compliance

Achieving and maintaining HIPAA compliance requires organizations to implement a structured, comprehensive approach that addresses all applicable regulatory requirements while establishing sustainable processes for ongoing compliance management. The following five essential steps provide a practical framework for organizations to develop effective compliance programs that protect patient information, meet regulatory expectations, and support business operations. These steps reflect both regulatory requirements and industry best practices derived from successful compliance implementations across diverse healthcare organizations.

Step 1: Appoint a HIPAA Privacy Officer and Security Officer if Required

Organizations must begin their compliance journey by appointing qualified individuals to serve as HIPAA Privacy Officer and, when required, a Security Officer (U.S. Department of Health and Human Services, n.d.-b; n.d.-c). The Privacy Rule mandates that all covered entities designate a Privacy Officer responsible for developing, implementing, and enforcing privacy policies and procedures. The Security Rule requires covered entities and business associates to designate a Security Officer who oversees the implementation of administrative, physical, and technical safeguards for electronic protected health information. These roles may be assigned to the same individual in smaller organizations, but each must have clearly defined responsibilities and sufficient authority to implement necessary compliance measures.

The Privacy Officer serves as the primary point of contact for patients, workforce members, and regulatory authorities regarding privacy matters. This individual must possess deep knowledge of the Privacy Rule requirements, excellent communication skills, and the ability to translate complex regulatory requirements into practical operational procedures. The Security Officer requires technical expertise in cybersecurity, risk management, and information systems to effectively implement and oversee security safeguards required by the Security Rule.

Both officers must receive appropriate training on HIPAA requirements and maintain current knowledge of regulatory developments, enforcement trends, and industry best practices. Organizations should provide these individuals with adequate resources, including training budgets, technology tools, and administrative support, to fulfill their compliance responsibilities effectively. The officers must also have direct access to senior leadership to ensure that compliance concerns receive appropriate attention and resources.

The Privacy Rule mandates that all covered entities designate a Privacy Officer responsible for developing, implementing, and enforcing privacy policies and procedures. The Security Rule requires covered entities and business associates to designate a ***Security Officer who oversees the implementation of administrative, physical, and technical safeguards for electronic protected health information.***

The Privacy Officer's responsibilities encompass developing and implementing privacy policies and procedures, conducting workforce training on privacy practices, managing patient rights requests, overseeing business associate relationships, and serving as the organization's privacy contact point. The Security Officer's duties include conducting risk analyses, implementing security safeguards, managing workforce security, overseeing information access controls, developing contingency plans, and ensuring ongoing security assessments.

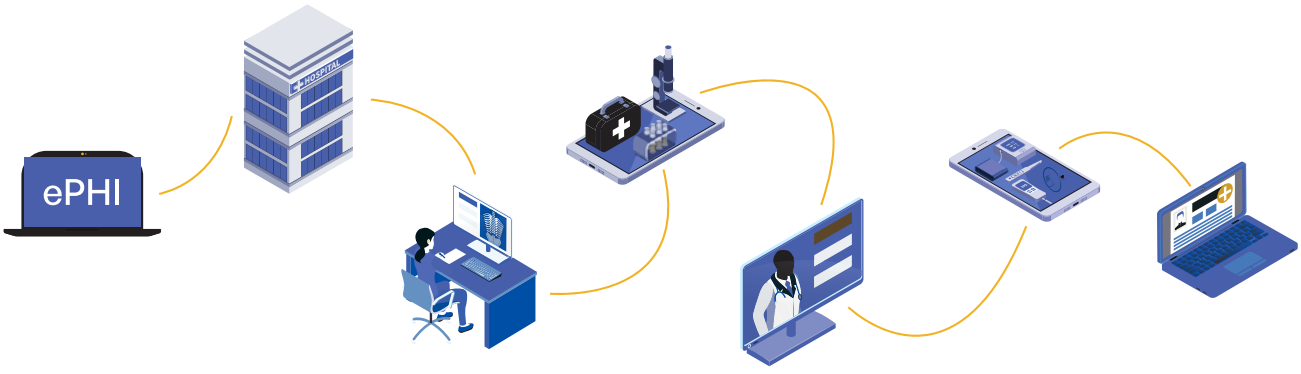
Step 2: Understand What PHI Is, Where and How It Is Used, and Stored

Organizations must develop a thorough understanding of what constitutes protected health information within their operations and create comprehensive inventories of how PHI is created, received, maintained, transmitted, and disposed of throughout the organization (U.S. Department of Health and Human Services, n.d.-a). Protected health information includes individually identifiable health information held or transmitted by covered entities or business associates in any form or media, whether electronic, paper, or oral. This encompasses medical records, billing information, and any other health information that could reasonably be used to identify an individual.

Organizations must develop a thorough understanding of ***what constitutes protected health information*** *within their operations and create comprehensive inventories of how PHI is created, received, maintained, transmitted, and disposed of throughout the organization.*

The PHI identification process requires examining all business processes, information systems, and data flows to identify every instance where PHI is handled. Organizations must understand the distinction between PHI and other types of information, such as de-identified health information or information that falls outside HIPAA's scope. The analysis must encompass both electronic and physical formats of PHI, including paper records, oral communications, and digital information stored in various systems.

Organizations must document where PHI is stored, including primary systems, backup storage, mobile devices, cloud services, and physical locations. This comprehensive mapping serves as the foundation for implementing appropriate safeguards and understanding the organization's risk exposure. The mapping process should document data flows between internal systems, external business associates, and third-party service providers to ensure comprehensive understanding of PHI movement throughout the organization's operations.Bitibust rero volupta temoloribus rem sunt viducip sandent



Organizations should categorize PHI based on sensitivity levels, access requirements, and regulatory protections to support implementation of appropriate security measures. Special attention must be paid to particularly sensitive categories of information, such as mental health records, substance abuse treatment records, and genetic information, which may be subject to additional regulatory protections beyond HIPAA requirements. Understanding these distinctions helps organizations implement appropriate access controls and safeguards.

Step 3: Understand That the Security Rule Consists of More Than Just Administrative, Physical, and Technical Safeguards and Implement Necessary Controls

The Security Rule requires implementation of administrative, physical, and technical safeguards, but organizations must understand that compliance extends far beyond these specific safeguards to encompass the General Rules that establish overarching requirements for protecting electronic protected health information (U.S. Department of Health and Human Services, 2024). The General Rules require covered entities and business associates to ensure the confidentiality, integrity, and availability of all electronic protected health information they create, receive, maintain, or transmit while protecting against reasonably anticipated threats and ensuring workforce compliance.

These General Rules create obligations that go beyond the specific safeguards outlined in the regulation, requiring organizations to implement proactive security measures that address evolving threats and vulnerabilities. Organizations must protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information, which may require security measures not explicitly specified in the administrative, physical, and technical safeguards sections.

Administrative safeguards form the foundation of security compliance, requiring organizations to establish security management processes, assign security responsibilities, implement workforce security procedures, manage information access, provide security awareness training, establish security incident procedures, develop contingency plans, and conduct periodic evaluations. These safeguards create the organizational structure and processes necessary for effective security management beyond basic policy requirements.

Physical safeguards protect electronic information systems and workstations from physical threats and unauthorized access, but organizations must consider threats beyond those explicitly addressed in the regulation. This includes protection against natural disasters, environmental hazards, and emerging physical security threats. Technical safeguards use technology to protect electronic protected health information and control access to it, but organizations must implement these measures in ways that address current cybersecurity threats and best practices.

The proposed Security Rule updates reflect this broader understanding of security requirements by eliminating the distinction between required and addressable implementation specifications and introducing specific technical requirements such as encryption, multi-factor authentication, and network segmentation. Organizations should prepare for these enhanced requirements by implementing comprehensive security programs that address both current requirements and anticipated future standards.

Step 4: Verify Data Breach Reporting Rules Applicable to Your Organization and Set Up Procedures for Notifying Individuals and HHS Office for Civil Rights

Organizations must establish comprehensive procedures for identifying, investigating, and responding to potential breaches of unsecured protected health information while understanding the specific notification requirements that apply to their operations (U.S. Department of Health and Human Services, n.d.-e). Breach notification requirements vary significantly based on the number of individuals affected, the nature of the breach, and the organization's location, making it essential for organizations to understand their specific obligations under both federal and state laws.

The HIPAA Breach Notification Rule requires covered entities to notify affected individuals, the Secretary of Health and Human Services, and in some cases the media when breaches of unsecured protected health information occur. For breaches affecting 500 or more individuals, organizations must notify affected individuals, HHS, and prominent media outlets serving the affected area within 60 days of discovery. For smaller breaches affecting fewer than 500 individuals, organizations must notify affected individuals within 60 days but may delay notification to HHS until the end of the calendar year.

*The HIPAA Breach Notification Rule **requires covered entities to notify affected individuals**, the Secretary of Health and Human Services, and in some cases the media when breaches of unsecured protected health information occur.*

Organizations must verify their specific reporting obligations to state attorneys general, as these requirements vary significantly by state and may impose additional notification obligations beyond federal requirements. Some states require immediate notification to state authorities, while others have different notification timelines, content requirements, or trigger thresholds. Organizations operating in multiple states must understand and comply with the most stringent applicable requirements to ensure comprehensive compliance.

Business associates have specific notification obligations when they discover breaches of unsecured protected health information, requiring them to notify covered entities within 60 days of discovery. The notification must include identification of each individual whose information was involved in the breach to the extent possible. Organizations must ensure their business associate agreements clearly specify these notification requirements and establish procedures for coordinating breach response activities.

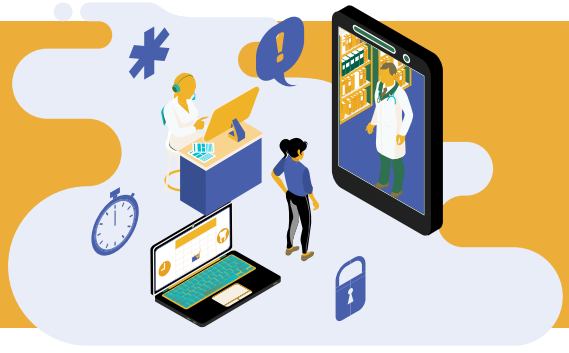
Breach determination requires organizations to assess whether incidents involving protected health information constitute reportable breaches under HIPAA. This assessment involves determining whether the information was secured through encryption or other methods, evaluating the likelihood that the information was compromised, and considering factors such as who accessed the information and whether it was further disclosed. Organizations should implement systematic breach assessment procedures that ensure consistent and appropriate breach determinations.

Step 5: Track Changes to HIPAA and Temporary Notices of Enforcement Discretion and Implement Those Changes

Organizations must establish systematic processes for monitoring HIPAA regulatory changes, enforcement developments, temporary enforcement discretion notices, and industry guidance to ensure ongoing compliance with evolving requirements (U.S. Department of Health and Human Services, 2024). This monitoring responsibility extends beyond formal rule changes to encompass enforcement guidance, regulatory interpretations, and temporary policy modifications that may affect compliance obligations.

The OCR periodically issues Notices of Enforcement Discretion that temporarily modify enforcement approaches for specific HIPAA requirements during emergencies or other exceptional circumstances. These notices became particularly important during the COVID-19 pandemic, when OCR provided temporary enforcement discretion for telehealth services and other healthcare delivery modifications. Organizations must monitor these notices, understand their applicability to their operations, and implement appropriate temporary modifications to their compliance programs.

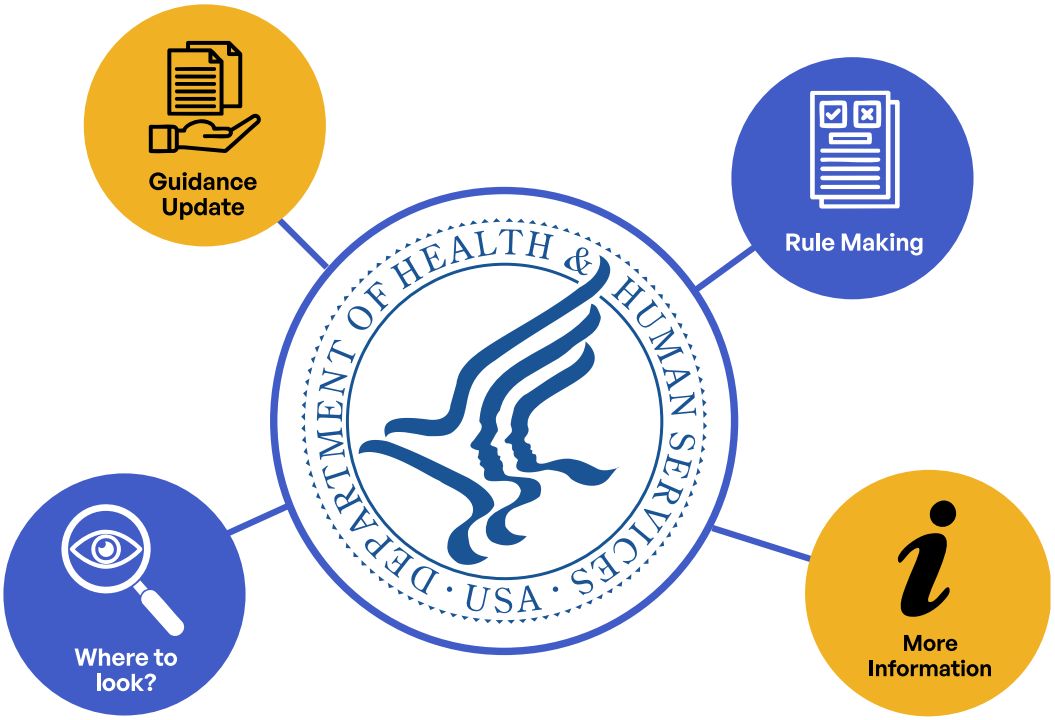
Regulatory changes to HIPAA can occur through formal rulemaking processes, enforcement guidance updates, and regulatory interpretations issued by HHS and its agencies. The proposed Security Rule updates represent the most significant regulatory changes since HIPAA's inception, requiring organizations to prepare for enhanced security requirements, mandatory implementation specifications, and new technical standards. Organizations must monitor the rulemaking process, assess the impact of proposed changes on their operations, and develop implementation plans for new requirements.



*Regulatory changes to HIPAA can occur through **formal rulemaking processes**, enforcement guidance updates, and regulatory interpretations issued by HHS and its agencies.*

Enforcement trends provide valuable insights into regulatory priorities and compliance expectations that may signal future regulatory changes or areas of increased scrutiny. Organizations should track enforcement actions, settlement agreements, and penalty assessments to understand common violation patterns and regulatory focus areas. This information helps organizations prioritize compliance investments, identify potential risk areas, and prepare for evolving enforcement approaches.

Organizations should also establish formal processes for reviewing regulatory updates, assessing their impact on current compliance programs, and implementing necessary changes to policies, procedures, and safeguards. This process should include regular review cycles, impact assessments, and implementation timelines that ensure timely compliance with new requirements. The monitoring program should encompass both proactive monitoring of regulatory sources and reactive assessment of changes that may affect the organization's compliance obligations.



The five essential steps outlined above provide a comprehensive framework for achieving and maintaining HIPAA compliance. Organizations must approach compliance as an ongoing process rather than a one-time project, with regular assessments, updates, and improvements to address evolving threats and regulatory requirements. Success requires commitment from senior leadership, adequate resource allocation, and sustained attention to compliance activities across all levels of the organization. These steps form the foundation for comprehensive compliance programs that protect patient information while supporting business operations in the complex regulatory environment.

How Kiteworks Supports HIPAA Compliance

Healthcare organizations require robust solutions that protect patient information while enabling efficient collaborative workflows and meeting stringent regulatory requirements. The Kiteworks Private Data Network (PDN) provides a comprehensive platform that addresses HIPAA Privacy, Security, and Breach Notification Rule requirements through automated end-to-end encryption, granular access controls, a hardened virtual appliance, and comprehensive audit logs.

1. Privacy Rule Compliance Through Advanced Access Controls

Kiteworks enables healthcare organizations to implement the minimum necessary standard through granular access controls that manage user permissions at file and folder levels. Role-based access controls assign specific access rights based on job functions, creating systematic information access aligned with organizational workflows. The platform's comprehensive auditing captures all user interactions with protected health information, providing documentation necessary for compliance assessments and regulatory investigations.

2. Security Rule Safeguards for Electronic Protected Health Information

The platform addresses Security Rule requirements through comprehensive administrative, physical, and technical safeguards. Kiteworks provides centralized user access management and activity monitoring tools that support administrative safeguard requirements. The platform enables secure remote access to protected health information from any device or location, reducing risks associated with storing sensitive information on physical devices.

Technical safeguards include multi-factor authentication, single sign-on integration, and granular access controls that provide multiple security layers. Integrity controls protect information through version control, file locking, and automated workflows that ensure only authorized users can modify sensitive data. Kiteworks ensures secure transmission through industry-standard encryption protocols, including SSL/TLS for data in transit and AES-256 for data at rest.

3. Breach Detection and Notification Capabilities

The platform supports Breach Notification Rule compliance through advanced monitoring tools that help organizations detect and respond to security incidents quickly. Real-time notifications and alerts, combined with comprehensive auditing capabilities, enable organizations to identify and investigate potential breaches rapidly. The platform's monitoring tools continuously assess system activities to identify potential security incidents before they escalate into reportable breaches.

4. Business Associate Collaboration and Omnibus Rule Compliance

Kiteworks facilitates secure communication and file sharing between covered entities and business associates, supporting Omnibus Rule requirements that extend Privacy and Security Rules to business associates and subcontractors. The PDN enables healthcare organizations to maintain oversight and control over protected health information shared with business associates while providing necessary collaboration capabilities.

5. Enhanced Protection for Genetic Information

Kiteworks addresses GINA compliance requirements by implementing content-defined zero-trust policies that ensure limited access to sensitive genetic information. The platform treats genetic information as protected health information with enhanced privacy controls that prevent unauthorized use or disclosure. Access controls are applied based on specific content types and sensitivity levels rather than relying solely on user credentials or network locations.

Through this integrated approach, Kiteworks enables healthcare organizations to confidently manage protected health information in complex, collaborative environments while maintaining strict compliance with all applicable HIPAA requirements.

References

HIPAA Journal. (2024). HIPAA compliance checklist. https://www.hipaajournal.com/hipaa-compliance-checklist/

HIPAA Journal. (2025). HIPAA violation fines – Updated for 2025. https://www.hipaajournal.com/hipaa-violation-fines/

Kiteworks. (n.d.). HIPAA compliance checklist. Retrieved July 10, 2025, from https://www.kiteworks.com/hipaa-compliance/hipaa-compliance-checklist/#topic9

U.S. Department of Health and Human Services. (n.d.-a). Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

U.S. Department of Health and Human Services. (n.d.-b). Summary of the HIPAA Privacy Rule. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

U.S. Department of Health and Human Services. (n.d.-c). Summary of the HIPAA Security Rule. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

U.S. Department of Health and Human Services. (n.d.-d). Covered Entities and Business Associates. https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html

U.S. Department of Health and Human Services. (n.d.-e). Breach Notification Rule. https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

U.S. Department of Health and Human Services. (2009, August 24). HITECH Breach Notification Interim Final Rule. https://hhs.gov/hipaa/for-professionals/breach-notification/laws-regulations/final-rule-update/hitech/index.html

U.S. Department of Health and Human Services. (2024, December 27). HIPAA Security Rule NPRM. https://www.hhs.gov/hipaa/for-professionals/security/hipaa-security-rule-nprm/index.html

https://www.govinfo.gov/app/details/CFR-2018-title45-vol1/CFR-2018-title45-vol1-sec164-408

https://www.hhs.gov/sites/default/files/breach-report-to-congress-2022.pdf

https://www.hipaajournal.com/hipaa-training-requirements/

Legal Disclaimer

The information provided in this report is for general informational purposes only and should not be construed as professional advice. Kiteworks makes no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability of the information contained in this report. Any reliance you place on such information is strictly at your own risk. None of the sponsoring or contributing organizations shall be liable for any loss or damage including without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising from loss of data or profits arising out of, or in connection with, the use of this report. Readers should consult with qualified legal counsel and cybersecurity professionals when addressing specific compliance requirements.

The data in this report was analyzed using AI and the content was generated with AI assistance. While AI enhances analytical capabilities, it can occasionally produce errors or biased information that should be considered when reviewing these findings.