WHITE PAPER

HIPAA Security Rule notice of proposed rulemaking: **organizational and documentation requirements**

The sixth white paper in a series addressing the specifics of organizational and documentation requirement changes in the NPRM.

Brittany Brown, BS, Health Information Management

RHIA | CHPS | CIPM (IAPP) | CCSK

COALFIRE® ADVISORY

Table of contents

Purpose

On December 27, 2024, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) issued a notice of proposed rulemaking (NPRM) to strengthen the cybersecurity protections of electronic protected health information (ePHI). This white paper provides a guide for Health Insurance Portability and Accountability Act (HIPAA) regulated entities (i.e., covered entities [CEs] and business associated [BAs]) to understand the proposed new requirements to the HIPAA Security Rule.

Due to the extensiveness of the proposed changes to the HIPAA Security Rule, this white paper is one of a series of six that divides the changes into the following subsections: (1) HIPAA Security Rule NPRM overview, (2) definitions, (3) administrative safeguards, (4) physical safeguards, (5) technical safeguards, (6) organizational requirements and documentation requirements. The series will go into depth with the proposed changes to the HIPAA Security Rule as outlined in the NPRM.

This white paper is the sixth in this series and provides information on organizational and documentation requirements.

Background

The HIPAA Security Rule was last updated in 2013, and, since then, both the healthcare environment and the cybersecurity threat landscape have experienced significant changes. The current NPRM has been put forward to help address these changes, and is essential to clarify compliance requirements for regulated entities and the courts, ensuring more consistent and effective enforcement of the legislation. HHS emphasizes the flexibility and scalability of the proposed updates, recognizing that these rules can be adapted based on an organization’s unique risk tolerance and the diverse nature of regulated entities, ranging from small healthcare practices to large hospital systems.

HHS recognizes the reality of ever-evolving cyber threats, acknowledging that “there is no such thing as a totally secure system that carries no risks to security.” However, the proposed updates are designed to be part of a comprehensive security management program, with an understanding that small practices may face greater risks due to limited resources. The requirements listed in the NPRM are the baseline, and regulated entities can implement additional safeguards as long as they do not conflict with the HIPAA Security Rule.

One critical issue identified by the OCR is that many organizations lack a clear understanding of where all the ePHI data they are entrusted to protect is located. Without this understanding, it is impossible to conduct a meaningful risk analysis. The first step in any effective security management strategy must be a clear inventory of the ePHI being collected, stored, and transmitted, as this knowledge forms the foundation for identifying vulnerabilities and implementing appropriate safeguards to protect patient data. The goal of the NPRM is to enhance organizations' ability to identify and track all locations of electronic protected health information (ePHI) by strengthening risk analysis requirements and promoting more comprehensive data inventory practices, thereby laying a stronger foundation for effective security measures and improved patient data protection.

The history and evolution of the HIPAA Security Rule

The HIPAA Security Rule, published in 2003 was designed to create a national standard for safeguarding ePHI through administrative, physical, and technical measures for CEs (e.g., health plans, healthcare clearinghouses, and healthcare providers) who electronically transmit health information. The HIPAA Security Rule standards require CEs to implement reasonable and appropriate safeguards to protect individually identifiable health information (IIHI) in electronic form. The standards were put into place to ensure the confidentiality and integrity of IIHI, protect against any reasonable anticipated threats or hazards to the security or integrity of IIHI (including unauthorized uses or disclosures), and ensure compliance with the administrative simplification provisions of HIPAA.

In 2013, the HIPAA Omnibus Rule was introduced, modifying the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health (HITECH) Act and the Genetic Information Nondiscrimination Act. The Omnibus Rule expanded the application of the Security Rule's administrative, physical, and technical safeguards BAs, holding them to the same standards as CEs. This change effectively broadened the scope of regulated entities to include BAs.

As published, the HIPAA Security Rule has utilized the legal language of "reasonable and appropriate" to give regulated entities flexibility when implementing security measures. Regulated entities must consider several factors when determining how to comply with these standards, including their size, complexity, and capabilities; their technical infrastructure, hardware, and software capabilities; the cost of security measures; and the likelihood and severity of potential risks to ePHI.

Why the update?

Given the recent, immense changes to the environment in which health care is provided, HHS has provided the following reasons for the NPRM:

- **Technological evolution**: Updates are necessary to address the significant advancements in technology since the 2013 HIPAA Omnibus Rule. As digital health tools, telemedicine, and cloud computing continue to evolve, the law must be updated to account for new methods of storing, transmitting, and securing ePHI, ensuring the HIPAA Security Rule remains relevant and effective in safeguarding sensitive data.
- **Cybersecurity threats**: The healthcare sector is increasingly targeted by cyberattacks, including ransomware, phishing, and data breaches. These attacks have become more sophisticated, highlighting the urgent need for stronger security measures to protect ePHI. The sharp rise in data breaches across the healthcare sector (Table 1) not only highlights a troubling trend but also serves as a stark warning: the current safeguards are no longer sufficient to protect sensitive health information in an increasingly digital environment. This surge in breaches underscores the urgent need for the enhanced cybersecurity strategies outlined in the NPRM, including advanced encryption, multi-factor authentication, and continuous monitoring. These measures are no longer optional but essential to safeguarding patient trust and maintaining the integrity of the healthcare system.
- **HHS and NIST guidelines**: To ensure comprehensive protection of ePHI, healthcare organizations must align with best practices outlined by HHS and the National Institute of Standards and Technology (NIST). While both organizations have published materials, it is apparent that a change in legislation is required to enforce adopting standard security best practices. By using these guidelines, healthcare entities can bolster their security frameworks, address emerging risks, and implement technical safeguards that mitigate vulnerabilities, ensuring the confidentiality and integrity of patient data.
- **Legislative intent**: The proposed updates aim to clarify the original intent of HIPAA, ensuring that the law is interpreted with a focus on safeguarding patient privacy and security in an ever-changing technological landscape. This ensures that courts and regulators uphold the spirit of the law, not just the specific language. By focusing on the underlying intent of the law, these updates promote more effective enforcement and protection of ePHI in today's dynamic healthcare environment.
- **Enforcement insights**: OCR has identified recurring gaps and weaknesses in healthcare security practices, which continue to pose risks to ePHI. These findings emphasize the need for continuous monitoring, regular risk analyses, and proactive remediation to address vulnerabilities before they can be exploited. By addressing these weaknesses, healthcare organizations can improve their overall security posture, ensuring compliance with HIPAA regulations and protecting patient data from emerging threats.

Breach data

HHS has reported HIPAA/HITECH breach data annually since 2009. The table below shows that data as reported to Congress. HHS used this data in creating the NPRM.

Year	Small breaches (fewer than 500 affected individuals)		Large breaches (500+ affected individuals)		Total	
	Breach count	Affected individuals	Breach count	Affected individuals	Breach count	Affected individuals
2018	63,098	296,948	302	12,196,601	63,400	12,496,549
2019	65,771	284,812	408	38,723,966	63,179	39,017,778
2020	66,509	312,723	656	37,641,403	67,165	37,954,126
2021	63,571	319,215	609	37,182,558	64,180	37,501,773
2022	63,966	257,105	626	41,747,613	57,592	42,004,718

Table 1: Breaches of PHI reported to Congress 2018 to 2022

Organizational and documentation requirements

While the current legislation is expansive, OCR's enforcement efforts and best practices for improving the cyber protections of ePHI have identified significant gaps. For instance, regulated entities have often misinterpreted the standards given as "addressable" as "optional." (Per HHS, "addressable" has never meant "optional;" all addressable standards must be satisfied.) With more frequent data breaches, cyberattacks, and disruptions caused by climate-related events, the healthcare sector is facing heightened challenges in securing ePHI. Additionally, the healthcare landscape has shifted significantly since the last update in 2013.

The NPRM was introduced to mitigate these gaps, and various current organizational policies, procedures, and practices may need to be revised to align with these changes. Therefore, it is essential to ensure that stakeholders are educated about the updated organizational and documentation requirements and their implications, so that the impact of the changes is fully understood and informed decisions about operations can be made.

NPRM updates to organizational and documentation requirements

The subsections below detail the key updates that the NPRM proposes to make to the HIPAA Security Rule organizational and documentation requirements, as well as examples of the standards in use.

General rules

The NPRM seeks to remove the concept of "addressable" throughout the HIPAA Security Rule. As a result, all organizational and documentation requirements are now classified required, and a regulated entity should use its risk analysis and management program to understand how to reasonably and appropriately implement measures to support the requirements. Please note, however, that the HIPAA Security Rule's organizational and documentation requirements are defined as a baseline, and HIPAA regulated entities can choose to implement additional requirements if they do not conflict with the HIPAA Security Rule.

HHS now requires that security measures must be documented in writing and implemented both for systems containing ePHI and for relevant electronic information systems. (The NPRM defines a relevant electronic information system as “an electronic information system that creates, receives, maintains, or transmits [ePHI] or that otherwise affects the confidentiality, integrity, or availability of ePHI.”) These required security measures must be reviewed and tested for effectiveness at least every 12 months, and whenever there is a change in the regulated entity’s environment or operations that may affect ePHI. Examples of this type of change can range from organizational acquisitions to changes in state law. baseline; regulated entities can choose to implement additional requirements if they do not conflict with the HIPAA Security Rule.

Business associate contracts or other arrangements

To address the risk and trends deficiencies in protections, the NPRM proposes to add an implementation specification to the business associate contracts and other arrangements standard that would require covered entities to update to business associate agreements include a provision for a business associate to report to the CE without unreasonable delay, but no later than within 24 hours of, its contingency plan activation. This proposal does not change the business associate's breach reporting obligations under the HIPAA Breach Notification Rule but ensures timely notification about the contingency plan activation. The CE and BA should negotiate terms of the form, content, or manner of the notice.

The example below provides an illustration of the standard in use, as well as relevant action items:

- **Standard in use example:** Regulated Entity *ABC*’s contracts with business associates currently state that notification must occur within 72 hours; additionally, the contracts do not specify which events, such as distributed denial-of-service (DDoS) attacks or other critical security incidents, should trigger such notification.
- **Action items**: Regulated Entity *ABC* should revise its business associate agreements to include clear provisions for reporting critical events, such as DDoS attacks, data breaches, or other incidents adversely affecting the confidentiality, integrity, or availability (CIA) of ePHI and relevant electronic information systems. The agreement should specify that notification of such events must occur within 24 hours of the activation of the contingency plan.

Requirements for group health plans

The NPRM proposes to update the implementation specifications under requirements for group health plans standard to require that group health plan documents obligate the plan sponsor, or any agent with access to ePHI, to implement the administrative, physical, and technical safeguards outlined in the HIPAA Security Rule. Additionally, the plan documents must include a provision requiring the plan sponsor to report to the group health plan no later than 24 hours after activating its contingency plan. The group health plan and plan sponsor may negotiate the form, content, and manner of the notification and include those details in their plan documents if they wish.

The example below provides an illustration of the standard in use, as well as relevant action items:

- **Standard in use example:** Regulated Entity *ABC*’s group health plan documents do not include the latest security rule enhancements, such as the requirement to implement MFA.
- **Action items**: Regulated Entity *ABC* needs to review and revise group health plan documents to ensure they include the most current administrative, physical, and technical safeguards required under the HIPAA Security Rule, ensuring the plan’s compliance with the latest security standards and that plan sponsors report within 24 hours of activating its contingency plan.

Documentation requirements

The NPRM proposes to clarify that regulated entities would be required to document the policies and procedures implemented to comply with the HIPAA Security Rule, including an explanation of how the entity considered flexibility in its approach, such as factors like size, complexity, infrastructure, costs, and risk when developing these policies. This documentation may be maintained in electronic form. Additionally, regulated entities would be required to document all actions, activities, and assessments required by the HIPAA Security Rule. The documentation must be updated at least once every 12 months and within a reasonable timeframe after modifying any security measures.

The example below provides an illustration of the standard in use, as well as relevant action items:

- **Standard in use example:** Regulated Entity *ABC*’s current enterprise policy mandates documentation updates every two years, which does not align with the HIPAA requirement for annual updates. Additionally, the policy does not define how flexibility in approach, considering factors like size, complexity, and risk, should be integrated into the development of policies and procedures.
- **Action items**: Regulated Entity *ABC* needs to revise its enterprise policy to require documentation updates at least annually and include a clear provision for defining flexibility in approach, based on factors such as size, complexity, infrastructure, costs, and risk.

Summary

The NPRM for the HIPAA Security Rule introduces significant changes to the framework for protecting ePHI, requiring regulated entities to implement comprehensive security measures which must be documented and periodically reviewed. With the removal of addressable standards, all safeguards are now mandatory, demanding a stricter compliance approach. Healthcare organizations must adapt to these updated requirements while managing risk in a complex and dynamic healthcare environment.

To effectively manage the new requirements and reduce the risks posed by the complex healthcare environment, organizations must adopt a Governance, Risk, and Compliance (GRC) program. A well-structured GRC program offers a balanced, structured, and scalable approach to building organizational processes to manage risk and comply with regulatory requirements while achieving business operational goals and objectives. This type of program helps organizations to ensure that they not only meet current legal and regulatory obligations but also to establish sustainable processes for addressing future challenges. By integrating risk management practices with operational goals, a GRC program helps healthcare organizations balance compliance with achieving broader business objectives, fostering a culture of security and compliance.

Appendix A: references

- The Notice of Proposed Rule Making § 164.314 Organizational Requirements
- The Notice of Proposed Rule Making § 164.316 Documentation Requirements

Appendix B: acronyms

Acronym	Term
BA	Business associate
CE	Covered entity
CIA	Confidentiality, integrity, and availability
ePHI	Electronic protected health information
GRC	Governance, risk, and compliance
HHS	U.S. Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
HITECH	Health Information Technology for Economic and Clinical Health Act of 2009
IIHI	Individually identifiable health information
MFA	Multi-factor authentication
NIST	National Institute of Standards and Technology
NPRM	Notice of proposed rulemaking
OCR	Office for Civil Rights

Table B-1: Acronyms

Legal disclaimer

This white paper is provided by Coalfire Systems, Inc. or its subsidiaries ("Coalfire") for informational purposes only. This white paper is the property of Coalfire and is protected by U.S. and international copyright laws. Unauthorized use, reproduction, or distribution of this white paper, in whole or in part, is strictly prohibited. Factual information included in this white paper has been taken from sources that Coalfire believes to be reliable, but its accuracy, completeness, or interpretation cannot be guaranteed. Information is current as of the date of this white paper only and is subject to change without notice. This white paper is provided "as-is" with no warranties, including any warranty of merchantability, fitness for a particular purpose, and non-infringement. Coalfire expressly disclaims all liability arising from or relating to the use of any information or material included in this white paper for any purpose, including any actions taken or not taken based on the contents of this white paper. You are solely responsible for making your own independent assessment of the information in this white paper and for the development, implementation, and execution of your information security program. For questions regarding any legal or compliance matters referenced in this white paper, you should consult your legal counsel, security advisor, or the relevant standard authority.

About the authors

Brittany Brown, BS HIM, RHIA | CHPS | CIPM (IAPP) | CCSK, *GRC Healthcare Consultant*

With a decade of information technology management and healthcare information management experience, Brittany is responsible for translating the complex requirements created by healthcare-related risk and compliance mandates into attainable, business-centric cyber solutions strategies.

Brittany's expertise spans a wide range of frameworks and standards, including NIST SP 800-53, HIPAA, MARS-E, EDE/DE, CMMC, and ISO 27001. Her hands-on experience in healthcare security risk analysis, policy development, and system security planning makes her a trusted advisor to clients navigating the evolving cybersecurity landscape. Brittany is also passionate about mentoring emerging professionals through the American Health Information Management Association (AHIMA), further demonstrating her commitment to advancing the field.

About Coalfire

The world's leading technology infrastructure providers, SaaS companies, and enterprises – including the top 5 cloud service providers and 8 of the top 10 SaaS businesses – rely on Coalfire to strengthen their security posture and secure their digital transformations. As the largest firm dedicated to cybersecurity, Coalfire delivers a comprehensive suite of advisory and managed services, spanning cyber strategy and risk, cloud security, threat and vulnerability management, application security, privacy, and compliance management. A proven leader in cybersecurity for the past 20 years, Coalfire combines extensive cloud expertise, advanced technology, and innovative approaches that fuel success. For more information, visit **Coalfire.com**.

WP_HIPAA Security Rule NPRM Definitions_05142025