WHITE PAPER

HIPAA Security Rule notice of proposed rulemaking: **definitions**

The third white paper in a series addressing the specifics of administrative safeguard 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 second in this series and provides information on definitions.

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

Modernization of definitions

When definitions in legislation are added, redefined, clarified, or expanded, it can have a significant impact on how the law is interpreted and applied. These changes are made for several reasons, including broadening or narrowing the scope of the law, clarifying ambiguities, adapting to technological or societal changes, and improving enforcement. As definitions are modernized, they directly affect how regulated entities must comply with the HIPAA Security Rule and how the law is enforced. Consequently, policies, procedures, and practices may need to be revised to align with these changes. In addition, it is essential to ensure that stakeholders are educated about the updated definitions and their implications so that they fully understand the impact of the changes and can make informed decisions in their operations.

New definitions

The list below provides new definitions to the HIPAA Security Rule as included in the NPRM, along with the proposed definition, its purpose, and an example of its use in context.

Term	Explanation	Example
Deploy	The addition of the word “deploy” would identify a specific type of implementation that requires a regulated entity to ensure that technical policies and procedures are implemented through the installation, configuration, and actual use of technology.	The technical safeguard of antimalware would be required to be deployed throughout the enterprise.
Implement	The addition of the word implement is to require that regulated entities not only have written policies and procedures in place for technical safeguards, but also to ensure that a safeguard is in place, in effect, and functioning as expected throughout the enterprise, as opposed to only some components of a regulated entity’s relevant electronic information systems.	The regulated entity would need to implement network segmentation by physically or logically separating systems that handle ePHI from other parts of the network.
Electronic information system	The addition of the term electronic information system is intended to provide clarity by explicitly defining the foundational concept of	The regulated entities network infrastructure that supports the

Term	Explanation	Example
	the systems to which safeguards must be applied. Without this definition, it was previously unclear which systems were covered under the HIPAA Security Rule requirement for safeguards. The proposed definition confines an "electronic information system" to an interconnected set of electronic information resources under the same direct management control that shares functionality. Under this definition, electronic information systems would generally include technology assets, hardware, software, electronic media, data, and information.	transmission and processing of ePHI. This would include servers, firewalls, switches, etc.
Multi-factor authentication (MFA)	The proposed rule defines the term MFA to mean "requirements for authenticating users' identities through verification of at least two of three categories of factors of information about the user." The NPRM proposes to add this term to establish MFA as the minimum implementation baseline required for regulated entities to meet the requirements of the HIPAA Security Rule. This MFA requirement provides enhanced security.	A regulated entity may require a user authenticate to access a healthcare application via username and password, followed by a token being sent to an application.
Relevant electronic information system	The addition of this term significantly expands the scope of HIPAA covered systems. The current definition focuses protections on electronic information systems that create, receive, maintain, or transmit ePHI. However, with the updated term, the scope now includes systems that may not directly interact with ePHI but still have the potential to affect the confidentiality, integrity, or availability (CIA) of ePHI. This broader scope ensures that any system, even those that support or influence ePHI workflows or infrastructure, is held to the same rigorous security standards to protect sensitive health information.	• A gift shop payment system in a hospital may affect the CIA of ePHI if not properly segmented from a system that interacts with ePHI. • A hospital's HVAC system could impact the availability of ePHI if servers are not efficiently cooled.
Risk	Adding a definition of the word "risk" to mean the extent to which the CIA of ePHI is threatened by a potential circumstance or event emphasizes the need to implement security measures based on the level of risk identified in a risk analysis..	A regulated entity may identify a risk to the availability of ePHI due to and instead of relying on standard backup protocols based on the amount of data being processed, the entity would implement a managed software for automated backup and recovery.
Technical controls	The addition of this term is intended to make clear the HHS' intent that "technical controls" means the "technical mechanisms contained in hardware, software, or firmware components used to protect the electronic information system that are primarily implemented and executed by the electronic information system to protect it and the data within the electronic information system." This was added to clarify the court's interpretation of technical policies and procedures as merely written documentation, rather than actual technical mechanisms implemented in systems. This distinction is crucial because the proper implementation of technical controls is essential to safeguarding the CIA of ePHI.	A regulated entity implements an encryption tool across its systems, configuring the encryption strength to meet current industry best practices, such as using AES-256 for data at rest and TLS 1.2 or higher for data in transit.
Technology asset	HHS proposes defining "technology asset" to mean "the components of an electronic information system, including but not limited to hardware, software, electronic media, information, and data." The intention behind adding this term is to identify that	When an organization conducts an inventory of technology assets it must include the components within the information system, as well as the functionality of those

Term	Explanation	Example
	the requirements of the HIPAA Security Rule apply to all components of electronic information systems.	components. For instance, if a regulated entity uses a cloud electronic health record (EHR) system, the entity's inventory must account for not only the cloud software, but also the computers and mobile devices accessing the software. Additionally, this includes any third-party services or applications that may interact with the system (e.g., backup software).
Threat	HHS proposes defining the term "threat" to mean "any circumstance or event with the potential to adversely affect the confidentiality, integrity, or availability of ePHI." The addition of this term meant to help in identifying threats, such as during a risk analysis, as the threats can exploit vulnerabilities in the regulated entities' information systems.	When conducting a risk analysis, a threat of a natural disaster such as a hurricane would require a regulated entity to backup information and systems to a geographically separate location.
Vulnerability	HHS proposes a definition of "vulnerability" similar to the NIST definition of "a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source." The addition this term is meant to form the basis for understanding the safeguards of risk analyses, patch management, and vulnerability management and scans.	A regulated entity undergoes a third-party risk analysis that detects a vulnerability in the configuration of its firewall settings. The firewall is not configured to fail-securely. In the event of a network failure, the firewall will not automatically block access and can leave the system and ePHI vulnerable to exploitation.

Table 2: New definitions in the NPRM

Clarified definitions

The table below includes the terms whose definitions are clarified by the NPRM, along with the proposed definition, its purpose, and an example of its use in context.

Term	Explanation	Example
Access	The current definition of the term "access" as "the ability or means necessary to perform a set of activities describing how a user may interact with a system resource." Where activities means "reading, writing, modifying, communicating data/information, or otherwise using any component of an information system," does not fully represent how users interact with information system components today. The proposal is to update the definition to include the activities a user or technology asset can do to access ePHI via deleting and transmitting data.	The regulated entity would also need to log the activities of deleting or transmitting ePHI.
Administrative safeguards	The current definition for administrative safeguards ("administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information") does not make it clear that	Regulated entities would need to conduct regular reviews of employee access to systems containing ePHI to ensure that only authorized personnel have access. This involves actively checking and adjusting access levels based on

Term	Explanation	Example
	administrative actions are included in addition to written policies and procedures. Furthermore, it does not specify that these safeguards should be regularly updated and reviewed. The proposed updates and clarifies this language.	role changes, terminations, or job duties.
Authentication	The current definition of authentication defines the process via a person, and does not include technology assets as a part of the authentication process. The proposed change to the definition of authentication would include technology assets, to more accurately define the roles that technology assets play in information systems.	Regulated entities would need to ensure that internet of things (IoT) devices are part of the enterprise authentication process. Authentication would need to occur in the network to ensure the devices are trusted and can safely interact with ePHI.
Availability	The current definition of availability could be perceived to limit the scope of availability to only authorized. The proposal is to expand availability to also include authorized technology assets that need to be able to access the ePHI to perform their intended functions.	Regulated entities would need to ensure that backup solutions are operational to be able to retrieve ePHI in the event of a system failure or data loss.
Confidentiality	The current definition of confidentiality could be perceived as requiring that information is not exposed to only unauthorized persons. The proposal is to expand the definition of confidentiality to include prohibiting the exposure or disclosure of ePHI to unauthorized technology assets.	Application programming interfaces (APIs) must be properly secured with encryption and authentication mechanisms to ensure that ePHI is not exposed to unauthorized parties or applications and prevent data leakage.
Password	The current definition of password defines a password as "a string of characters" but does not define what constitutes a "character." The proposal is to define characters as letters, numbers, spaces, and other symbols.	A regulated entity may require a password policy to enforce the concept of password complexity, which technically requires passwords to be configured of a combination of uppercase and lowercase letters, numbers, spaces, and special symbols.
Physical safeguards	The HHS proposes to update the current definition of a physical safeguard to clarify that the "policies and procedures" referred to in the definition are those that are specifically related to physical measures. This will reduce minor inconsistencies with the language of the HIPAA Security Rule and clarify that the HHS has always intended that "physical safeguard" apply to any location where a regulated entity potentially possesses ePHI.	A regulated entity needs to ensure network closets are restricted to only authorized personnel through use of measures such as locked doors, security badges, biometric authentication, and surveillance cameras to monitor and control physical access to the closet.
Security or Security measures	The current definition defines security or security measures as part of the information system, instead of something that may be applied or done to a system to protect the CIA of ePHI. Updating the definition to clarify that that security or security measures includes mechanisms both in information systems and applied to information systems helps support a defense-in-depth approach to security.	A regulated entity deploys firewall technology and intrusion detection systems to protect the information system.
Security incident	The current definition does not make it clear that a security incident may be the result of two different types of behavior: those related to the unauthorized direct access, use, disclosure,	An unauthorized user tries to access ePHI by exploiting a vulnerability in the system but is

Term	Explanation	Example
	modification, or destruction of an information system or those that may interfere with the operations of the information system. The proposed definition clarifies this point and also makes clear that a security incident exists regardless whether the attempt to affect or interfere with the information system was successful.	unsuccessful. The incident must still be investigated, documented, and reported to internal security and privacy leads, as it demonstrates a potential threat that could impact the security of the system.
Technical safeguards	The current definition does not include technical controls. Updating the definition helps support the understanding that technical safeguards not only include policies, procedures, and technology but also the implementation of technical controls.	An organization uses role-based access to technically restrict access. Access would be restricted based on role and the principle of minimum necessity.
User	HHS proposes to simplify and clarify the current definition of "user" by removing the reference to an entity. Since the term "person" already covers entities, including "entity" in the definition of "user" is redundant and could cause confusion.	HHS states this is a technical correction and does not change the interpretation of the term.
Workstation	The current definition of "workstation" does not reflect the current technology environment where smart phones, tablets, virtual desktops, and other devices may be used to access ePHI. The updated definition provides additional examples of workstations such as server, virtual device, and a mobile device (e.g., a table or smart phone).	A mobile device would need to be encrypted, and other protective measures implemented.

Table 3: Clarified definitions in the NPRM

Modified definitions

The table below includes the terms whose definitions are modified by the NPRM, along with the proposed definition, its purpose, and an example of its use in context.

Term	Explanation	Example
Information system	The current definition is modified to clarify the scope of an information system and define the difference between an electronic information system and information system. An information system, generally, includes hardware, software, data, communications, and people.	A technology asset, such as a cloud-based her, may be included in several different regulated entities information systems. For instance, a hospital and a healthcare provider may all interact with the information system and have control over the ePHI within the system.
Malicious software	The current definition does not meet the standard definition of malicious software today as malicious software does more than damage and disrupt a system. The modified definition defines malicious software as software or firmware intended to perform an unauthorized action or activity that will have an adverse impact of the electronic information system and/or the CIA of ePHI.	A keylogger installed on a workstation that records keystrokes, including login credentials for accessing ePHI systems.

Table 4: Modified definitions in the NPRM

Summary

The modernization of definitions within the HIPAA Security Rule is a necessary step toward strengthening the security of ePHI in today's increasingly complex technological landscape. These updates reflect the environment of healthcare organizations today, which utilize a range of devices, systems, and cloud-based technologies. These technological assets must be implemented and deployed to ensure the confidentiality, integrity, and availability of ePHI. For regulated entities, this means revisiting their security policies and ensuring that they are aligned with the latest regulatory requirements. In practice, this will require a combination of updated technology, new security measures, and ongoing employee training to ensure compliance.

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 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, ultimately fostering a culture of security and compliance.

Appendix A: references

- The Notice of Proposed Rule Making § 164.304 Definitions.

Appendix B: acronyms

Acronym	Term
API	Application programming interface
BA	Business associate
CE	Covered entity
CIA	Confidentiality, integrity, and availability
CMS	Centers for Medicare & Medicaid Services
EDR	Endpoint detection and response
EHR	Electronic health record
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
IoT	Internet of things
MFA	Multi-factor authentication
NIST	National Institute of Standards and Technology
NPRM	Notice of proposed rule making
OCR	Office for Civil Rights
PHI	Protected health information
PII	Personally identifiable information

Table 5: 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