WHITE PAPER

HIPAA Security Rule notice of proposed rulemaking: **technical safeguards**

The fifth white paper in a series addressing the specifics of technical 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 fifth in this series and provides information on technical safeguards.

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

HIPAA Security Rule technical safeguards

The current technical safeguards in the HIPAA Security Rule consist of five standards: (1) access control, (2) audit controls, (3) integrity, (4) person or entity authentication, and (5) transmission security.

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.) In addition, the healthcare landscape has shifted significantly since 2013, with the transition to digital environments increasing the risk to ePHI and with the cost of implementing technology solutions, such as encryption, decreasing.

Recent breaches, including those due to insufficient monitoring of information systems, lack of security measures to protect ePHI during transmission, unencrypted laptops, and personnel accessing medical records without a job-related purpose, underscore these gaps in technical safeguard compliance. HHS also reviewed breaches beyond healthcare when developing the NPRM, noting that threat actors often gain access to networks by compromising user accounts and exploiting insufficient network segregation.

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 technical safeguards and their implications, so that they the impact of the changes is fully understood and informed decisions about operations can be made.

NPRM updates to technical safeguards

The subsections below detail the key updates that the NPRM proposes to make to the HIPAA Security Rule technical safeguards, 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 technical safeguards are now classified as 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 required safeguards. Please note, however, that the HIPAA Security Rule's technical safeguards are defined as a baseline, and HIPAA regulated entities can choose to implement additional safeguards 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.

Access control

The NPRM proposes to clarify the standard for access control by requiring a regulated entity to not only establish policies and procedures but also implement those technical controls for relevant electronic information systems to ensure role-based access is restricted to authorized users and technology assets. The NPRM would add a requirement to assign a unique identifier to each technology asset, as well as each user, to track unauthorized activity and require regulated entities to adhere to the minimum necessary standard for administrative access. To ensure proper access control and security, users should have two separate accounts: one for non-administrative access and another for administrative functions. The non-administrative account would be used for regular tasks and to access general information, while the administrative account would be reserved for tasks requiring elevated privileges, such as system configurations or user management. Entities may further enhance controls with privilege access management systems.

A regulated entity would also be required to also establish written and technical procedures for obtaining the necessary ePHI during an emergency. It must deploy technical controls that terminate an electronic session after a period of inactivity, considering factors such as user access privileges and system type. Additionally, technical controls should disable or suspend access after a certain number of unsuccessful authentication attempts, tailored to the type of user or technology asset. Entities would be required to implement segmentation of relevant electronic information systems to mitigate security risks. Finally, the effectiveness of these procedures and controls should be reviewed and tested at least once every 12 months or in response to operational changes, with adjustments made based on risk analysis, to define the reasonableness and appropriateness of the technical controls in place.

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

- **Standard in use example:** Regulated Entity *ABC* has identified a gap in its user access management system. Privileged users currently use a single account for both administrative functions and regular non-administrative tasks.
- **Action items**: Regulated Entity *ABC* needs to update its policies and procedures to require privileged users to have separate accounts for administrative tasks and non-administrative functions. Additionally, the entity must implement technical controls to enforce this separation, ensuring that administrative access is restricted and

monitored, while non-administrative tasks are performed with standard access privileges. These controls should be integrated into the identity management system.

Encryption and decryption

The NPRM proposes redesignating the encryption and decryption implementation specification to a standard in the HIPAA Security Rule, due both to its importance in reducing the risk to ePHI and to the increasing affordability of encryption solutions. Under the proposal, a regulated entity would be required to configure and implement technical controls to encrypt and decrypt all ePHI in compliance with prevailing cryptographic standards. “Prevailing cryptographic standards” here refers to widely accepted encryption decryption standards as recommended by authoritative sources to ensure the confidentiality, integrity, and availability (CIA) of ePHI at time of the entity’s risk analysis. The entity would be required to ensure that any encryption solution adopted meets these standards, as determined through its risk analysis and risk management plan.

The NPRM also requires that regulated entities encrypt ePHI both at rest and in transit, with only limited exceptions. Such exceptions include:

1. For technology assets that do not currently support encryption to prevailing cryptographic standards. In this case, the regulated entity would need to establish and implement a written migration plan to upgrade to technology that supports encryption.
2. When ePHI is transmitted in response to an individual’s request for access. If the individual requests unencrypted access, the entity must inform them of the risks involved, and the exception only applies if system security is not compromised. This exception does not apply when the individual receives ePHI through technology controlled by the entity, such as a patient portal.
3. In emergencies or other circumstances that make encryption infeasible, with compensating controls implemented according to the contingency plan.
4. For ePHI created, received, maintained, or transmitted by FDA-authorized medical devices. The NPRM proposes three separate exceptions based on when the devices was submitted to the FDA and whether the devices is still supported by the manufacturer.

If any of the four exceptions apply, the regulated entity must document the exception and implement reasonable compensating controls. These compensating measures must be reviewed and approved by the designated Security Official.

The regulated entity must also review and test the effectiveness of the encryption controls at least once every 12 months, or whenever significant environmental or operational changes occur, and modify them as necessary based on the findings.

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

- **Standard in use example:** Regulated Entity *ABC* uses an application that does not adhere to accepted encryption standards due to the use of TLS 1.1. While the application is essential for operations, an upgrade to a more secure version is not available at this time.
- **Action items**: Regulated Entity *ABC* should develop a plan to transition off the current software once an upgrade becomes available or find alternative solutions that comply with current encryption standards. In the meantime, the entity should implement compensating controls, such as enhanced monitoring, access restrictions, network segmentation, frequent security audits, and encryption gateways, to mitigate potential security risks. These controls should be documented and reviewed regularly. The entity must ensure the exception process is followed, including justifying the deviation, implementing compensating measures, and reassessing the situation until full

compliance is achieved. The designated Security Official must approve the exception and review it regularly to ensure continued compliance with encryption requirements.

Configuration management

To reduce the opportunity for a cyberattack and the potential for the compromise of ePHI, the NPRM proposes adding a standard for configuration management. Under this proposed standard, a regulated entity would be required to establish and deploy technical controls to secure its electronic information systems and technology assets, including workstations, in a consistent manner. This involves setting and maintaining a baseline level of security for each system and technology asset. The entity would also be required to protect against malicious software, such as viruses and ransomware, by implementing appropriate technical controls like antimalware or endpoint detection and response (EDR) systems. Additionally, unnecessary software, as defined by the organization's risk analysis, should be removed if it is not required for operations. Finally, operating systems and software must be configured and secured, and unnecessary network ports should be disabled.

The entity's risk analysis should guide the implementation and assessment of these technical controls, ensuring their reasonableness and appropriateness. A regulated entity is required to review and test the effectiveness of the technical controls outlined in the configuration management standard at least once every 12 months.

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 vulnerability test identified that unnecessary ports, including port 23 for Telnet, were open on the network. It was identified that port 23 is not required for the organization's operations and poses a security risk.
- **Action items**: Regulated Entity *ABC* should disable port 23 and any other unnecessary open ports, conduct regular port reviews, and update network configuration procedures to ensure only essential ports are accessible.

Audit trail and system log controls

To improve regulated entities' understanding of and compliance with the HIPAA Security Rule's auditing requirements, the NPRM proposes updating and renaming the current standard to provide more specificity. A regulated entity would be required to assess its risk analysis and additional organizational factors, such as current infrastructure and security capabilities, to determine appropriate audit controls. The entity would also be required to deploy either or both technology assets and technical controls to record and identify activities within its relevant electronic information systems to ensure it can address activity that presents a risk to ePHI. This includes monitoring, in real-time, all relevant electronic information system activity, not just systems that create, receive, maintain, or transmit ePHI. Such activities include, but are not limited to, detecting unauthorized access and activity and alerting workforce members accordingly.

Additionally, the entity would be required to retain records of all system activities in accordance with its policies. The scope of activities to be recorded includes, but is not limited to, creating, accessing, receiving, transmitting, modifying, copying, or deleting ePHI, as well as creating, accessing, receiving, transmitting, modifying, copying, or deleting relevant electronic information systems and the information therein. The regulated entity must review and test the effectiveness of the audit controls at least once every 12 months, or whenever significant environmental or operational changes occur, and modify them as necessary based on the findings.

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

- **Standard in use example:** Regulated Entity *ABC* has system and application logs being fed into its monitoring system; however, alerts are not being generated and sent to team members for unauthorized activities or anomalies. This gap in real-time alerting hinders the ability to quickly identify and respond to potential security incidents.

- **Action items**: Regulated Entity *ABC* needs to configure the monitoring system to generate real-time alerts based on predefined criteria for unauthorized activities. The entity will also need to establish a process for ensuring alerts are promptly sent to the appropriate team members for timely response.

Integrity

To improve the effectiveness of the existing integrity standard and help prevent the alteration and destruction of ePHI regardless of source, the NPRM proposes to modify the current standard for clarity. The NPRM proposes that a regulated entity must now implement technical controls (as opposed to the previous “policies and procedures”) to protect ePHI from unauthorized alteration or destruction both at rest and in transit. These controls should be reviewed and tested for effectiveness at least once every 12 months or whenever there are environmental or operational changes.

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

- **Standard in use example:** Regulated Entity *ABC* currently lacks the technical capability to verify that electronically exchanged health information has not been altered. Specifically, there is no use of a hashing algorithm that meets the necessary requirements to ensure data integrity.
- **Action items**: Regulated Entity *ABC* should implement a hashing algorithm that meets the required standards to verify the integrity of electronically exchanged health information. Additionally, the entity should integrate this capability into other existing health IT systems and test its effectiveness regularly

Authentication

The NPRM proposes to redesignate and rename the current authentication standard to reflect the standard’s broad purposes. Under the NPRM, a regulated entity would be required to implement technical controls (as opposed to the previous “implement procedures”) that verify the identity of individuals or technology assets seeking access to ePHI and relevant information systems. These controls should align with the entity’s information access management policies and procedures, including requirements for users to adopt unique passwords. Default passwords must be changed, and unique passwords should adhere to current authoritative recommendations. Additionally, password sharing among personnel should be prevented.

In addition to unique identification, regulated entities would be required to deploy MFA across all technology assets in their relevant electronic information systems. The implementation of MFA must align with the entity’s risk analysis. The NPRM provides for three exceptions to the MFA requirement:

1. The first exception applies when a technology asset does not support MFA. In such cases, the regulated entity must create a written plan to migrate ePHI to systems that support MFA and complete the migration within a reasonable timeframe.
2. The second exception applies when MFA is infeasible due to emergencies or other significant disruptions to the entity’s electronic systems. In these situations, the entity must implement compensating controls as part of its contingency plan and emergency access procedures.
3. The third exception applies to devices authorized by the FDA for marketing. These devices, which are authorized after March 29, 2023 and are supported by their manufacturer, would be subject to compensating controls. The regulated entity must ensure that compensating controls for expectations are reasonable, appropriate, and reviewed and approved by the entity’s Security Official. If the compensating controls are found to be ineffective, new controls must be implemented.

The regulated entity must review and test the effectiveness of the authentication controls at least once every 12 months or whenever significant environmental or operational changes occur and modify them as necessary based on the findings.

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

- **Standard in use example:** Regulated Entity *ABC* has implemented technical controls to secure access to ePHI, including the use of MFA. However, during a recent risk analysis, it was identified that MFA is configured to allow one-time passwords (OTPs) being sent via text message to users for authentication. This practice was flagged as a potential vulnerability. Given the large scale of the organization and the high number of users accessing sensitive systems, the risk of SMS-based OTPs being intercepted or compromised is significant. SMS-based OTPs are more susceptible to interception, SIM-swapping, and other security threats, making them an inadequate solution for an organization of this size and complexity.
- **Action items**: Regulated Entity *ABC* should disable the use of SMS-based OTPs for MFA to mitigate the risk of interception and SIM-swapping attacks based on recent risk analysis results. The entity should enforce the use of application-based OTP solutions across all systems for more secure authentication. Additionally, the organization should update its MFA configuration, communicate the changes to workforce members, and provide training to ensure smooth adoption of the new authentication method.

Transmission security

The NPRM proposes to clarify the existing transmission security standard by requiring regulated entities to deploy technical controls to protect ePHI from unauthorized access during transmission over electronic communication networks. These controls should be reviewed and tested for effectiveness at least once every 12 months or whenever there are environmental or operational changes.

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

- **Standard in use example:** Regulated Entity *ABC* has implemented encryption protocols during transmission over its networks. However, it was identified during a risk analysis that encryption keys are not rotated.
- **Action items**: Regulated Entity *ABC* should implement a regular key rotation policy and automate the process, where possible, through tools such as a key management system (KMS). Additionally, the entity should evaluate and update key management practices in response to changes in technology or security threats.

Vulnerability management

To address the potential for a bad actor to exploit publicly known vulnerabilities, the NPRM proposes a new standard for vulnerability management. This standard would require a regulated entity to deploy, in alignment with its patch management policies, technical controls to identify and address vulnerabilities in its electronic information systems. These controls include conducting automated scans on all components of relevant electronic information systems at least every six months, or sooner depending on the entity's risk analysis.

The NPRM would also require the entity to test the effectiveness of its scanning technology at least annually or in response to environmental or operational changes. Additionally, regulated entities should continuously monitor authoritative sources for known vulnerabilities and take prompt action to ensure remediation. Penetration testing by qualified individuals must be conducted at least once a year. The entity would also be required to implement timely software patches and critical updates. For obsolete systems, the entity must establish safeguards to mitigate vulnerabilities until upgrades or replacements can occur.

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

- **Standard in use example:** Regulated Entity *ABC* currently uses an unsupported operating system due to a legacy application that cannot be migrated or replaced at this time.
- **Action items**: Regulated Entity *ABC* needs to implement strict access controls to limit user access to the unsupported operating system, alongside deploying additional technical safeguards such as network segmentation and monitoring tools to mitigate security risks. Continuous monitoring of vulnerabilities and emerging threats related to the unsupported system is essential. Additionally, the entity should develop and execute a detailed plan to upgrade or replace the legacy application and operating system within a defined timeline.

Data backup and recovery

The NPRM proposes adding a new standard for data backup and recovery, emphasizing the liability of regulated entities in restoring systems after a data breach. This new standard would require a regulated entity to deploy technical controls to create and maintain exact, retrievable copies of ePHI and to ensure that such backups are no more than 48 hours older than the ePHI in its systems. The entity must deploy real-time monitoring and alert systems for backup failures and error conditions that record the success, failure, and any error conditions of backups. Additionally, the entity is required to test and document the effectiveness of backups at least monthly by restoring a representative sample of ePHI, verifying the ability to access data remotely.

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

- **Standard in use example:** Regulated Entity *ABC* underwent a risk analysis that identified some systems that process ePHI currently undergo weekly backups.
- **Action items**: Regulated Entity *ABC* must revise its backup schedule to ensure that backups for all systems processing ePHI are completed at least every 48 hours. The entity should deploy technical controls to automate the backup process and ensure compliance with the 48-hour rule.

Information systems backup and recovery

The NPRM proposes adding a new standard for backup and recovery. This standard would require a regulated entity to deploy technical controls to create and maintain backups of its relevant electronic information systems. The entity is required to review and test the effectiveness of these controls at least every six months or in response to changes. Instead of testing every system, the entity would be able to review log files and test a representative sample of its backups, with the extent of testing determined by the size and complexity of the systems in use.

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

- **Standard in use example:** Regulated Entity ABC currently tests backups only once annually, and there is no defined structure or process in place to determine which system backups are tested, leading to potential gaps in backup validation.
- **Action items**: Regulated Entity *ABC* should establish a structured backup testing process that ensures a representative sample of systems and data are tested at least every six months. The entity should also implement a documented procedure that outlines which backups will be tested, considering system complexity and operational changes, to ensure comprehensive backup validation.

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, conduct annual penetration testing, perform automated vulnerability scans every six months, and implement MFA across all systems accessing ePHI. All these measures must be documented and periodically reviewed. With the transition from addressable to mandatory standards, regulated entities must ensure that all technical safeguards are fully implemented, regularly tested, and updated to reflect changes in the healthcare landscape, demanding a stricter compliance approach. Healthcare organizations must adapt to these updated requirements while managing risk in a complex and dynamic healthcare environment. Throughout the NPRM, the Department of HHS emphasizes that a thorough risk analysis should drive the implementation of technical controls to ensure they are reasonable and appropriate for the size and complexity of the organization. This highlights the critical importance of conducting a risk analysis, as it helps entities tailor security measures based on their unique risks and operational 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 § 164.312 Technical Safeguards

Appendix B: acronyms

Acronym	Term
BA	Business associate
CE	Covered entity
CIA	Confidentiality, integrity, and availability
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
KMS	Key management system
MFA	Multi-factor authentication
NIST	National Institute of Standards and Technology
NPRM	Notice of proposed rulemaking
OCR	Office for Civil Rights
OTP	One-time password

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 responsiblefor 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**.

Copyright © 2025 Coalfire. All rights reserved. The information in this document is subject to change at any time based on revisions to applicable regulations and standards. Any forward looking statements are not predictions and are subject to change withoutnotice. Coalfire is not responsible for any errors or omissions.

WP_HIPAA Security Rule NPRM Definitions_05142025