WHITE PAPER

# HIPAA Security Rule notice of proposed rulemaking: **administrative safeguards**

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 third in this series and provides information on administrative 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 administrative safeguards

The current administrative safeguards in the HIPAA Security Rule consist of eight standards: (1) security management process, (2) assigned security responsibility, (3) workforce security, (4) information access management, (5) security awareness and training, (6) security incident procedures, (7) contingency plan, and (8) evaluation.

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.) Also, gaps have been noted in risk analyses where relevant electronic information systems that do not process ePHI but are still relevant to the confidentiality, integrity, and availability (CIA) of the system have been omitted. Additionally, regulated entities are not ensuring that the ePHI they entrust to BA is protected through appropriate administrative safeguards.

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

# NPRM updates to administrative safeguards

The subsections below detail the key updates that the NPRM proposes to make to the HIPAA Security Rule administrative 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 administrative safeguards 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 required safeguards. Please note, however, that the HIPAA Security Rule's administrative 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 [CIA] of ePHI.") These required security measures must be reviewed and tested for effectiveness at least every 12 months and when 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.

## Technology asset inventory

As OCR's investigations frequently find that organizations lack sufficient understanding of where all the ePHI entrusted into their care is located, HHS proposes a standard that would require regulated entities to conduct and maintain an accurate and comprehensive written technology asset inventory and network map of the electronic information system and all technology assets that may affect the CIA of ePHI. HHS states that an accurate technology asset inventory and network map serve as the foundation for conducting accurate and thorough risk analyses. The inventory must contain the identification, version, person accountable for, and location of each of the assets or information system components.

Network maps should identify where technology assets are located, such as the regulated entities' server room or cloud infrastructure. Network maps must also identify any technology assets utilized to create, receive, maintain, or transmit ePHI to a BA. Furthermore, the network map must clearly show the flow of ePHI at entry and exit points and detail how the information system is accessed outside of its secure boundary.

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 maintains a technology asset inventory. The asset inventory includes servers, laptops, applications, and other technology assets that process ePHI. However, upon inspection, smart infusion pumps were used in critical care and other care units. The smart infusion pumps are configured to report directly into the electronic health record (EHR). The smart infusion pump is configured to allow bi-directional communication to reduce manual programming errors as recommended by the Joint Commission. Despite their role in patient care, these devices are not properly included in the enterprise asset inventory and are tracked differently across various hospital units.
- **Action items**: Regulated entity *ABC* needs to integrate the smart infusion pumps into the enterprise asset inventory. The information technology (IT) team needs to ensure that the devices are patched and maintained properly to address security vulnerabilities. Additionally, *ABC* must update its policies and procedures to include internet of things (IoT) devices like infusion pumps in the technology asset inventory and train staff on the security risks associated with improperly managed IoT devices that affect ePHI.

## Risk analysis

### Risk analysis standard

Regulated entities are already required to conduct an accurate and thorough risk analysis under the current HIPAA Security Rule. However, when HHS conducted audits of 166 CEs and 41 BAs in 2016 and 2017 regarding compliance with selected provisions of the HIPAA Rules, including the required implementation specifications for risk analysis, they found that most regulated entities failed to implement the HIPAA Security Rule requirements for risk analysis and risk management. Accordingly, the NPRM proposes to elevate the requirement to conduct a risk analysis from an

implementation specification to a standard and to more explicitly state the requirements for an accurate, comprehensive risk analysis. Such requirements include several key steps:

- Review the technology asset inventory and network map to identify where ePHI is created, received, maintained, or transmitted.
- Identify any potential threats to the CIA of ePHI and assess vulnerabilities in their systems that could impact ePHI.
- Create an assessment, document the security measures in place to protect ePHI, determine the likelihood of threats exploiting these vulnerabilities, and assess the potential impact if a threat successfully exploits a vulnerability.
- Assess the risk level for each identified threat and vulnerability and evaluate the risks associated with business associate agreements based on the verification obtained from those BAs.

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 been relying on a third party for its annual risk assessments. Upon reviewing the reports, it was discovered that instead of performing a true risk analysis, the assessments merely mirrored a HIPAA gap analysis focused on ensuring compliance with the HIPAA Security Rule. For example, the report indicated Regulated Entity *ABC* follows the HIPAA Security Rule and ensures compliance by enforcing complex password requirements for user accounts accessing ePHI systems. The password policy mandates a minimum of 8 characters with a mix of upper and lowercase letters, numbers, and special characters. However, upon review of the Active Directory system, it was identified that privileged users follow the same global password complexity requirements, despite their elevated access to sensitive systems and data. The risk is that privileged accounts are more likely to be targeted by attackers, and the password requirements for these accounts are not stringent enough to protect them from sophisticated attacks.
- **Action items**: Regulated Entity *ABC* must conduct a comprehensive risk analysis to evaluate the threats and vulnerabilities to its information systems, specifically focusing on the CIA of ePHI. The entity should revise its password policy to enforce more stringent requirements for privileged user accounts, such as longer passwords (e.g., 12 characters or more) and the enforcement multi-factor authentication. In addition, the organization should perform regular audits of privileged accounts to ensure these measures are properly enforced and to identify any additional security gaps

  The entity should also establish a formalized monitoring process, in line with NIST guidelines, to continuously assess the security posture of its systems. This monitoring should support the risk management program by prioritizing asset risks and conducting periodic analysis reviews to ensure that asset portfolios remain current and relevant. Ongoing risk analyses should be conducted as part of a cyclic process to proactively manage emerging threats and vulnerabilities, with regular adjustments based on up-to-date risk assessments.

## New and emerging technologies request for information

The NPRM highlights the need for regulated entities to address emerging technologies like quantum computing, artificial intelligence (AI), and virtual and augmented reality in healthcare. While these technologies have the potential to transform healthcare in various ways, regulated entities must also assess the associated risks and implement strategies to secure them. The HIPAA Security Rule, along with the proposed updates, is technology-neutral, meaning that when changes occur, the risk analysis process and management program serve as essential tools. These tools help assess the potential risks and vulnerabilities to the CIA of ePHI created, received, maintained, or transmitted. Furthermore, the NIST AI Risk Management Framework is recommended as a valuable resource for understanding and managing the risks, effects, and potential harms associated with AI technologies.

## Evaluation

The NPRM proposes to require that technical and nontechnical evaluations be in writing and performed to determine whether a change in the regulated entity's environment or operations may affect the CIA of ePHI. Unlike a risk analysis, which looks at the entity's entire enterprise regularly or in response to operational changes, an evaluation focuses on a specific change before it occurs. Evaluations must be conducted within a reasonable time period before implementing the change. The evaluation process should be conducted in accordance with the regulated entity's risk management plan. Examples of changes can include adopting new technology, updating systems, identifying new threats, mergers, security incidents, or changes in relevant laws.

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

- **Standard in use example:** Regulated Entity *ABC* finance team has introduced new software to assist in reporting revenue cycle metrics. The software was reviewed by the finance team for functionality requirements and was approved by the accounting department for purchase. While the finance team did review and approve the software, IT was not notified of the software vendor before the software was introduced into the information system. As a result, the IT department discovered that the new software utilized a lot of memory and was causing systems that process ePHI to crash.
- **Action items**: Regulated Entity *ABC* must conduct a written evaluation prior to any changes in the environment or operations that may affect the CIA of ePHI. The evaluation must be documented and include potential vulnerabilities, compatibility concerns, and security measures to mitigate identified risks. Additionally, the entity should implement a formal process to ensure all system changes or upgrades are reviewed and evaluated by both technical and nontechnical teams before proceeding. This process should also be aligned with the organization's risk management plan.

## Patch management

The NPRM proposes a new patch management standard requiring a regulated entity to implement written policies and procedures for identifying, prioritizing, acquiring, installing, evaluating, and verifying the timely installation of patches, updates, and upgrades throughout the electronic information systems. If a system is obsolete and cannot be upgraded or replaced, additional safeguards, such as enhanced access restrictions, modification of configuration files, disabling unnecessary services or features, and/or extended service agreements should be implemented and documented as exceptions to mitigate vulnerabilities. Critical risks should be addressed within 15 days, high risks within 30 days, and other updates or upgrades should be performed within a reasonable timeframe as determined by the entity's policies.

There are two exceptions to this proposed standard: (1) if a patch, update, or upgrade is not available to address the risk or (2) if the patch, update, or upgrade would adversely affect the CIA of ePHI. For these exceptions to apply, they must be documented, and the regulated entity must implement reasonable and appropriate compensating controls.

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 a patch management program with detailed policies and procedures in place. However, a recent penetration test report highlighted a high-risk vulnerability that has not been resolved, with the report dating back over 60 days. The IT director explained that addressing the vulnerability would disrupt communication with critical software, and a support ticket has been opened with the vendor to resolve the issue.
- **Action items**: Regulated Entity *ABC* must ensure proper documentation of any exceptions, such as when a patch is unavailable or adversely impacts ePHI, and implement reasonable compensating controls in those

cases. Additionally, the patch management process should be reviewed annually to ensure continued compliance with the requirements.

## Risk management

The NPRM proposes elevating the implementation specification for risk management to a standard. This proposed standard would require a regulated entity to establish and implement a plan for reducing the risks identified through its risk analysis activities. This includes documenting and implementing a written risk management plan that is updated every 12 months and in response to its risk analysis. The plan should prioritize risks identified in the entity's risk analysis and emphasize that security measures should be implemented promptly to address the risk.

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 a written risk management plan that details risk analyses that are required to be conducted annually. However, the plan lacks a formal requirement for prioritizing risks based on the criticality of each risk. As a result, there is no clear framework for addressing the most pressing risks first, which could lead to inefficient or delayed implementation of security measures to protect ePHI.
- **Action items**: Regulated Entity *ABC* needs to update its risk management plan to include a formal requirement for prioritizing risks based on their criticality and potential impact on ePHI. The plan should also specify that security measures will be implemented promptly based on this prioritization. Furthermore, the plan should be reviewed and updated not only annually but also in response to significant changes identified in the risk analysis or operational environment.

## Sanction policy

Sanction policies, and training personnel on those policies, are a great tool for maintaining workforce awareness of the accountability and consequences of not complying with security policies and procedures. As such, the NPRM proposes elevating the implementation specification for sanction policy to a standard. This proposed standard would require a regulated entity to establish written sanction policies and procedures for workforce members who fail to comply with the regulated entity's own policies and procedures. The documentation must be reviewed every 12 months. Regulated entities must apply appropriate sanctions against personnel who fail to comply with security policies and procedures. When personnel are sanctioned, it must be documented, and such documentation must include the circumstances for why the sanction was applied.

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 a general sanction policy in place, but it does not document the specific events or details around an employee sanction when it occurs. The organization relies on verbal communications regarding violations, and there are no formal records or logs of the personnel involved, procedural steps taken, or the final outcome. For instance, when a workforce member accesses ePHI without proper authorization, a warning is given, but no written record is created to track the violation or the reasoning behind the warning.
- **Action items**: Regulated Entity *ABC* needs to update its sanction policies and procedures to require written documentation of all events that lead to a sanction. This should include details such as the personnel involved, the specific violation, the procedural steps taken, the time frame, the reason for the sanction, and the final outcome. The updated policy should ensure that all sanctions, from warnings to termination, are thoroughly documented and reviewed at least every 12 months for consistency and effectiveness in preventing future violations.

## Information system activity review

To help address the significant challenges of detecting and preventing data leakage initiated by malicious users or whether any ePHI has been used or disclosed in an inappropriate manner, the NPRM proposes elevating the existing implementation specification for information system activity review to a standard. This proposed standard would require a regulated entity to document policies and procedures for regularly reviewing activity records in its electronic information systems, including both people and technology assets. This review should cover the entire system and its components, such as workstations. The frequency of the review would depend on the type of information in the system and the specific reports or logs. The review process must be documented, and the retention of audit trails is based on what is considered reasonable and appropriate for each report or log. The entity would also be required to respond to any known or suspected security incidents based on the review. The information system activity review policies and procedures would be required to be reviewed and tested 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* has all information systems logs being fed into a security information event management (SIEM) system. The SIEM provides an overview of activity within the information system and helps in identifying potential security threats. However, upon review, it was noted that the security operations center (SOC) team reviews logs on an ad hoc basis, without a formal schedule or process for prioritizing certain types of logs over others based on their criticality or potential risk. Additionally, the documentation of when and why specific logs were reviewed is not consistently maintained, which makes it difficult to track the review process or respond to security incidents effectively.
- **Action items**: Regulated Entity *ABC* needs to update its policies and procedures to ensure that the SOC team reviews logs consistently and on a scheduled basis. The review process should be based on the type of information in the system, with a clear prioritization based on risk levels. Logs must be reviewed at regular intervals and documented to ensure traceability. The regulated entity should test and revise its policies and procedures for log reviews annually to ensure ongoing compliance and effectiveness.

## Assigned security responsibility

OCR's enforcement experience has found that, in practice, many regulated entities follow informal, undocumented policies and procedures for assigning security responsibility. As such, the NPRM proposes modifying the assigned security responsibility standard to require a regulated entity to document, in writing, the security official responsible for establishing and implementing policies and procedures and deploying technical controls. The same individual may serve as both the Privacy Officer and Security Officer. The overall security responsibility would be required to be assigned to one person, with additional responsibilities delegated to teams or other roles depending on the organization's size and complexity.

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 assigned a personnel member with ultimate security responsibility for the organization. This individual is responsible for approving security policies and overseeing the overall security strategy. However, the role is not fully defined or clearly outlined in a job description, and the broader organization is not well-informed about who holds security responsibilities or the extent of their role. As a result, the personnel member's duties and authority in relation to security may not be fully understood or recognized by other employees.
- **Action items**: Regulated Entity *ABC* needs to update its security policies and job descriptions to explicitly define the role and responsibilities of the security official. The job description should clearly outline the individual's duties in establishing and implementing security policies, procedures, and technical controls. Furthermore, the

organization should ensure that all employees are aware of who holds security responsibilities and the extent of their authority.

## Workforce security

The NPRM proposes to update the standard and implementations specifications for workforce security to clarify the actions required of a regulated entity to ensure workforce members have access to only the ePHI they need to perform their assigned functions. Regulated entities would be required to establish written policies and procedures that ensure workforce members have appropriate access to ePHI and relevant electronic information systems, while preventing unauthorized access. These policies must include clearance procedures for granting and revoking access. Termination procedures must also be documented and require access to be terminated as soon as possible, but no later than one hour after employment or a contract ends. Additionally, regulated entities would be required to notify other entities within 24 hours if a workforce member's access to ePHI, or relevant systems, changes or is terminated. Finally, a regular review and testing of these security policies and procedures must occur 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* has policies and procedures in place for workforce clearance, which require access termination within 24 hours. However, the policies do not currently address the requirement for notifying other entities when a workforce member's access to ePHI or relevant systems is terminated. Additionally, there are issues with maintaining access management for systems outside of the regulated entity's main information system, such as the claims filing system, where access control is not well documented or easily monitored.
- **Action items**: Regulated Entity *ABC* needs to update the policies and procedures to indicate access must be terminated within 1 hour and to notify other systems, such as the claims filing system, within 24 hours. The regulated entity should conduct an audit of all systems, outside of the information system, where personnel access ePHI. Where appropriate, the regulated entity should consider system integration to reduce the overhead of access management. The updated workforce security policies and procedures should be reviewed and tested for effectiveness at least every 12 months.

## Information access management

The NPRM proposes updates to the information access standard and implementation specifications that ensure that regulated entities implement recommendations and best practices for securing ePHI. A regulated entity would be required to have written policies and procedures that are tested every 12 months for effectiveness for authorizing access to ePHI and relevant electronic information systems consistent with the HIPAA Privacy Rule. These policies should detail the procedures for granting and revising access to ePHI and electronic information systems based on the role and function of each asset and user, including role-based access controls. The regulated entity would also be required to establish standards for granting access and ensure that formal authorization from the appropriate authority is provided before granting access to ePHI or relevant systems. Additionally, the identities of users and technology assets must be verified prior to system access, with multi-factor authentication (MFA) requirements in place, and a regulated entity must also establish written policies and procedures that ensure the electronic information systems are segmented, limiting access to ePHI to authorized users.

Additionally, the implementation specification for isolating healthcare clearinghouse functions would be modified to require healthcare clearinghouses that are part of a larger organization establish written policies and procedures to safeguard ePHI and relevant electronic information systems from unauthorized access by the larger organization.

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

- **Standard in use example**: Regulated Entity *ABC* operates a healthcare clearinghouse that is part of a larger organization. However, the healthcare clearinghouse is not segmented because it uses the same IT infrastructure and network as other departments within the organization. It was identified that employees from other departments, due to their role, such as medical biller, can obtain unauthorized access to parts of the healthcare clearinghouse network where the ePHI is stored.
- **Action items**: Regulated Entity *ABC* needs to segment the network subsystems for the clearinghouse so personnel from the larger organization are unable to access the ePHI. Additional technical safeguards, such as detailed access control lists, should be implemented to prevent unauthorized access to the clearinghouse system by medical billers or other employees from the larger organization. Policies and procedures should be generated to ensure safeguards are implemented to prevent unauthorized access from the larger organization.

## Security awareness training

The NPRM proposes to rename and redesignate the security awareness and training standard and to add information clarifying the methods and purpose of training. As such, security awareness training would be mandatory for all workforce members to ensure they can effectively protect ePHI and information systems in accordance with their roles. The training must cover key areas such as written policies and procedures, identifying and reporting security incidents, written policies, and procedures for accessing the regulated entity's electronic systems, and managing passwords. Training should be completed within 30 days of hire and repeated every 12 months, with additional training provided for new systems like EHRs, while ongoing reminders are required to reinforce security responsibilities and address emerging threats. The regulated would be required to  must document that training has been provided and include records of ongoing reminders.

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 an annual security awareness program that all personnel are required to undergo annually. Upon review, it was identified that while policy requires annual training there is no real oversight to ensure training is conducted in a timely manner. The existing program also lacks ongoing reminders and documentation to ensure training has been reinforced regularly throughout the year.
- **Action items**: Regulated Entity *ABC* needs to implement a formal oversight process to ensure that all workforce members complete security awareness training within the required timeframes. *ABC* should consider using alerts and notifications available in the current learning management system. Additionally, *ABC* should establish ongoing periodic reminders and refresher sessions to reinforce the workforce's security responsibilities and address emerging security threats.

## Security incident procedures

Security incident procedures have often been found lacking in OCR enforcement engagements, failing to meet the purpose and intent for responding to security incidents. HHS recommends following NIST guidance (NIST Special Publication [SP] 800-61) for managing these incidents. To help reduce the amount and negative consequences of security incidents, the NPRM proposes to modify the existing regulatory text to require a regulated entity develop written policies and procedures for responding to security incidents, including how personnel report incidents and how the regulated entity will respond upon detection and notification. The incident response plans must also outline how and when BAs report incidents. Additionally, the entity would be required to test and revise these response plans annually, document the results, and modify the plans based on testing outcomes and evolving circumstances.

To mitigate the harmful effects of security incidents, the proposed regulations would require regulated entities to identify and remediate the root causes of security incidents, including eradicating malicious software or inappropriate materials from relevant electronic systems. The regulated entity is required to develop and maintain documentation of

investigations, analyses, mitigation, and remediation efforts related to known or suspected incidents. This documentation, including verbal incident reports, must be retained for 6 years from the creation date.

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 maintains a security incident response plan that aligns with NIST SP 800-61. The entity tests the plan annually with stakeholders and response teams. However, upon review, the plan does not include guidelines on how BAs should report suspected or known incidents, including the timeline for required notification. Additionally, the entity's response procedures do not outline a systematic process for how the entity should respond to incidents reported by BAs, this can lead to confusion during a real investigation for suspected or confirmed incidents.
- **Action items**: Regulated Entity *ABC* needs to revise its security incident response plan to explicitly define the reporting requirements and timelines for BAs in the event of suspected or confirmed incidents. Additionally, the entity must establish a structured process for handling incidents reported by BAs to ensure clarity and coordination during an investigation. Once the plan is updated, it should be tested to incorporate lessons learned and ensure alignment among all parties, including BAs, in their response efforts.

## Contingency plan

Recent cyber incidents, including ransomware, have highlighted the lack of adequate planning and resilience in healthcare infrastructure, with many regulated entities unable to fully recover from such incidents. To address this gap, the NPRM proposes modify the contingency plan standard such that regulated entities would be required to establish written contingency plans that include policies and procedures for responding to emergencies affecting electronic information systems (e.g., fires, system failures, natural disasters, or security incidents). These plans must include a criticality analysis to assess and document the importance of electronic information systems and technology assets, prioritizing their restoration in case of disruption. Additionally, written data backup procedures are required to ensure accurate copies of ePHI and to verify the success of those backups. Systems and data restoration would be required to occur within 72 hours for critical systems and in accordance with the criticality analysis. Emergency mode operation procedures must also be documented. Finally, regulated entities must review and test their contingency plans annually, document the results, and make necessary adjustments based on test outcomes.

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 a contingency plan that identifies systems as critical due to the processing of ePHI, but it has not conducted a business impact analysis to assess the overall importance of information system components. As a result, the order of restoration is not clearly documented, which could lead to delays in recovering the most essential systems first. The lack of prioritization for restoration could negatively impact the entity's ability to recover quickly and efficiently.
- **Action items**: Regulated Entity *ABC* needs to conduct a business impact analysis to assess and document the criticality of its electronic information systems and technology assets. The entity must establish a clear order of restoration based on this analysis and update the contingency plan accordingly. Additionally, the plan should be tested regularly to ensure the prioritization of systems is effective and any potential gaps are identified.

## Compliance audit

As audit activities form important components of a robust cybersecurity program, the NPRM proposes a new standard for compliance audit that requires regulated entities to perform and document a compliance audit with each standard and implementation specification of the HIPAA Security Rule at least once every 12 months. This audit can be conducted internally or by a third party; however, to ensure objectivity and maintain the integrity of the audit, it is considered best

practice to have the audit be independent from the information security management team. This approach helps ensure unbiased results and a more accurate assessment of compliance.

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 monitors compliance with the HIPAA Security Rule on an ongoing basis but does not conduct a formal, documented audit annually. While the entity regularly reviews some security protocols, there is no independent, comprehensive audit to assess compliance with all relevant standards in the HIPAA Security Rule.
- **Action items**: Regulated Entity *ABC* needs to implement a formal, documented annual compliance audit for all relevant standards and implementation specifications of the HIPAA Security Rule. The audit should be conducted either internally or by a third party, with a clear separation from the information security management team to maintain objectivity. The entity must also ensure that audit results are documented, and any compliance gaps are addressed in a timely manner.

## Business associate contracts and other arrangements

The NPRM proposes several modifications to the HIPAA Security Rule to provide greater assurance that BAs and their subcontractors are protecting ePHI because a subcontractor to a BA is also a BA. These updates would require regulated entities to obtain a written agreement, such as a business associate agreement, that the BA will comply with the HIPAA Security Rule. In addition, written verification from BAs at least once every 12 months confirming that they have implemented the technical safeguards required by the HIPAA Security Rule would also be required. Such verification should include a written analysis of the BA's electronic information systems conducted by an individual with expertise in cybersecurity and ePHI protection. This individual may be a member of the CE's or BA's workforce or an external party. Additionally, the verification must be accompanied by a certification from an authorized individual at the BA confirming that the analysis has been completed and is accurate.

Additionally, a regulated entity may allow a BA to act as its designated security official. However, even when delegating actions, activities, or assessments required by the HIPAA Security Rule, the regulated entity remains liable for ensuring compliance with all applicable provisions of the HIPAA Security Rule.

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 business associate agreements in place with all BAs but has not been obtaining written verification annually regarding the implementation of technical safeguards as required by the HIPAA Security Rule.
- **Action items**: Regulated Entity *ABC* needs to establish a process to obtain annual written verification from BAs, including an analysis of their electronic information systems by a qualified individual. The regulated entity should maintain documentation of the verification and certification to ensure ongoing compliance with the HIPAA Security Rule.

# Summary

The NPRM for the HIPAA Security Rule introduces significant changes to the framework for ePHI. Such changes include requiring regulated entities to implement comprehensive security measures, such as compliance audits, workforce security, information access management, and incident response procedures, all of 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, ultimately fostering a culture of security and compliance.

# Appendix A: references

The Notice of Proposed Rule Making § 164.308 Administrative safeguards

# Appendix B: acronyms

| Acronym | Term |
|---|---|
| AI | Artificial intelligence |
| 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 |
| MFA | Multi-factor authentication |
| NIST | National Institute of Standards and Technology |
| NPRM | Notice of proposed rulemaking |
| OCR | Office for Civil Rights |
| PII | Personally identifiable information |

*Table B-1: Acronyms*

# Legal disclaimer



## 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, CMMC, EDE/DE, 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