Published on *The National Law Review* https://natlawreview.com

NIST Publishes Final "Cybersecurity Resource Guide" on Implementing the HIPAA Security Rule

Article By:

Christopher D. Taylor

Jennifer J. Hennessy

In an important development for HIPAA-regulated entities looking for practical assistance in understanding, implementing, and enhancing compliance with the HIPAA Security Rule, the National Institute of Standards and Technology (NIST) has finalized its comprehensive guidance, Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide (Resource Guide). This release follows the initial draft that NIST published for public comment in July 2022 and builds on NIST's foundational 2008 publication. The updated Resource Guide comes at the heels of the U.S. Department of Health and Human Services (HHS) releasing voluntary performance goals to enhance cybersecurity across the health sector last month and a Department-wide Cybersecurity strategy for the health care sector in December of 2023.

As a technology-neutral framework, the HIPAA Security Rule recognizes the diversity in the size, complexity, and capabilities of regulated entities, offering a flexible and scalable approach to safeguarding electronic protected health information (ePHI). Acknowledging that no single compliance strategy fits all organizations, the Resource Guide presents an extensive set of guidelines that entities may adapt in part or in full to strengthen their cybersecurity posture and achieve compliance with the HIPAA Security Rule. Moreover, the Resource Guide is structured to cater to various organizational needs and maturity levels in cybersecurity practices. It emphasizes that risk assessment and risk management processes are crucial to a regulated entity's compliance with the HIPAA Security Rule and the protection of ePHI.

Below is an overview of the content covered by the Resource Guide:

Considerations When Applying the HIPAA Security Rule

Perhaps most helpful is that NIST has broken each HIPAA Security Rule standard down by key activities that a regulated entity may wish to consider implementing, adding a detailed description, and providing sample questions to guide entities in their compliance efforts. This detailed guidance for each HIPAA Security Rule standard will be helpful for regulated entities struggling to adopt it with only the language in the HIPAA Security Rule and HHS guidance on the same.

In an accessible, tabular format, the Resource Guide outlines considerations for implementing the HIPAA Security Rule, highlighting:

- **Key Activities:** Actions typically associated with the security functions suggested by each standard.
- **Description:** Expanded explanations of these activities, detailing strategies for implementation.
- **Sample Questions:** Thought-provoking questions for self-assessment, aimed at gauging whether the standard has been adequately implemented. Negative responses to these questions should prompt further action to ensure compliance.

As an illustrative example, consider the standard on Security Incident Procedures, which mandates the implementation of policies and procedures to address security incidents. A key activity highlighted is “Developing and deploying an incident response team or other reasonable and appropriate response mechanism.” To assist entities in evaluating their readiness and implementation of this standard, NIST provides sample questions such as:

- Do members of the team have adequate knowledge of the organization’s hardware and software?
- Do members of the team have the authority to speak for the organization to the media, law enforcement, and clients or business partners?
- Has the incident response team received appropriate training in incident response activities?

To further aid organizations seeking to implement the HIPAA Security Rule, NIST also updated its Cybersecurity and Privacy Reference Tool (CPRT). The CPRT displays HIPAA Security Rule regulations, complemented with direct links to further NIST tools and resources for enhanced understanding and implementation.

Risk Assessment Guidelines

The Risk Assessment Guidelines section of the Resource Guide provides a methodology for conducting a risk assessment. The HIPAA Security Rule requires that all regulated entities “[c]onduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate” and then “[i]mplement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.” This is known as the security risk analysis and risk management plan, respectively. The results of the security risk analysis should enable regulated entities to identify appropriate security controls for reducing risk to ePHI. NIST’s guidance with respect to risk assessments is similar to previous HHS guidance provided at the Guidance on Risk Analysis and Security Risk Assessment Tool:

1. **Prepare for the Assessment**. Understand where ePHI is created, received, maintained, processed, or transmitted. This must include all parties and systems to which ePHI is transmitted, including remote workers, external service providers, and medical devices that process ePHI.
2. **Identify Realistic Threats**. Identify potential threat events and sources, including (but not limited to) ransomware, insider threats, phishing, environmental threats (e.g., power failure), and natural threats (e.g., flood).
3. **Identify Potential Vulnerabilities and Predisposing Conditions**. Identify vulnerabilities or conditions that can be exploited for the threats identified in Step 2 to have an impact.

4. **Determine the Likelihood of a Threat Exploiting a Vulnerability**. For each threat identified in Step 2, determine the likelihood of a threat exploiting a vulnerability. A low, moderate, or high-risk scale is commonly used but not required.
5. **Determine the Impact of a Threat Exploiting a Vulnerability**. The regulated entity should select an impact rating for each identified threat/vulnerability pair and may consider how the threat event can affect the loss or degradation of the confidentiality, integrity, and/or availability of ePHI. Example impacts would include an inability to perform business functions, financial losses, and reputational harm. Again, a low, moderate, or high-risk scale is commonly used but not required.
6. **Determine the Level of Risk**. The level of risk is determined by analyzing the overall likelihood of threat occurrence (Step 4) and the resulting impact (Step 5). A risk-level matrix can be helpful in determining risk levels for each threat event/vulnerability pair.
7. **Document the Results**.

Similar to previous HHS guidance, NIST reminds regulated entities that the risk assessment is an ongoing activity, not a one-off exercise. The assessment must be "updated on a periodic basis in order for risks to be properly identified, documented, and subsequently managed." The cybersecurity landscape is ever-evolving, with threats morphing and new vulnerabilities emerging even as existing ones are mitigated. Additionally, changes in an organization's operations, such as the introduction of new policies or technologies, can alter the likelihood and impact of potential threat events. This dynamic context underscores the necessity for risk assessments to be periodically revisited and updated. Such regular updates ensure that risks are accurately identified, documented, and managed in a timely and effective manner, aligning with the organization's evolving risk profile and enhancing its cybersecurity posture.

Moreover, failure to have a thorough and up-to-date risk assessment is one of the top failures documented by HHS in resolution agreements with regulated entities. Therefore, regulated entities should take this opportunity to determine when its last risk assessment was conducted, ensure the risk assessment meets previous HHS guidance, and consider the NIST guidance in this Resource Guide as well.

Risk Management Guidelines

NIST states that the Risk Management Guidelines introduce a "structured, flexible, extensible, and repeatable process" that regulated entities may utilize for managing identified risks and achieving risk-based protection of ePHI. The regulated entity will need to determine what risk rating poses an unacceptable level of risk to ePHI, given the regulated entity's risk tolerance and appetite. Ultimately, the regulated entity's risk assessment processes should inform its decisions regarding the implementation of security measures sufficient to reduce risks to ePHI to levels within organizational risk tolerance.

To illustrate, consider a scenario where an organization identifies a high risk to ePHI from ransomware attacks, characterized by both a high likelihood and a high impact. Upon implementing critical security measures—namely, Response and Reporting, Data Backup Plan, and Disaster Recovery Plan—the organization reassess and significantly lowers the risk level from "High" to "Low." Although the *likelihood* of such an attack remains high, the *impact* is now considered low due to these proactive measures, aligning the risk with the organization's risk tolerance.

Conclusion

NIST’s Resource Guide should serve as an essential resource for HIPAA-regulated entities, offering guidance on risk assessment, management, and compliance with the HIPAA Security Rule. In leveraging the Resource Guide, organizations can maintain robust protection for ePHI and adapt to changes in the cybersecurity landscape.

In addition to the Resource Guide itself, NIST has also provided supplementary content on its website to further assist HIPAA-covered entities and business associates with strategies to improve their cybersecurity in specific areas including Telehealth/Telemedicine, Mobile Device Security, Medical Device Security, Cloud Services, Incident Handling/Response, and others.

National Law Review, Volume XIV, Number 52