NEW STANDARDS FOR HIPAA:

Proposed Changes & How You Can Prepare

AHEAD

On January 6th 2025, the Department of Health and Human Services issued a notice of proposed rulemaking (NPRM) to solicit comment on its proposal to modify the Security Standards for the Protection of Electronic Protected Health Information ("Security Rule") under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act).

The key drivers of this proposed rule change are:

> Significant changes in healthcare, including the use of new and emerging technologies
>
> Ever-increasing security breaches and cyberattacks
>
> Observations resulting from compliance investigations and court decisions

Many of the concerns driving this proposed rule change align closely with existing controls defined within the NIST Cybersecurity, NIST Risk Management, and NIST Privacy frameworks. This suggests that organizations that have adopted these security and privacy control frameworks, or those that have achieved Health Information Trust Alliance (HITRUST) compliance, may be ahead of this 'pending curve;' however, it is safe to assume that all healthcare organizations would be affected at varying degrees.

A Look AHEAD

The proposed rule boasts nearly four hundred pages of changes that include a broad range of security, risk management, and privacy topics.

Some of the notable changes include:

> Data Protection and Access Control: Enhanced data protection controls, including more clearly defined data protection requirements for encryption, authentication, access controls, user training, and the use of AI systems specifically.
>
> Continuous Monitoring and Detection: Timely detection of anomalous behavior and issues that could indicate a breach or security issue, and the inclusion of AI systems and other emerging technologies in monitoring and detection capabilities.
>
> Incident Response and Recovery: Responding to incidents involving PHI requires effective detection, communication, and recovery plans. Enhanced requirements with specified RTO/RPO and annual documented remediation plans are proposed. This may expand reporting or breach notification processes as well as disaster and cyber recovery initiatives. For AI-related incidents, recovery plans may include validating that AI models are not compromised prior to full restoration.
>
> Data Sharing and Interoperability: Enhanced security measures as they pertain to Supply Chain Risk Management and Access Control can be expected, in addition to a stringent review of Business Associate Agreements (BAAs) and confirming that they reflect new responsibilities for handling ePHI under the new rule.
>
> AI Governance and Risk Management: Ensuring AI systems interacting with ePHI are subject to comprehensive risk assessments, clear governance, and strong oversight, expanding the scope for existing Data Governance programs.
>
> Increased Scope and Frequency of Assessment and Audit Activity: The rule changes propose requirements for more frequent vulnerability scans, penetration testing, program audits, and security control assessments.

Prepare for Agility – Our Recommendations

The proposed rule change would significantly alter the scope of existing cybersecurity and privacy programs for regulated entities. In response to these potential changes, the key is early preparation and agility. The following steps provide an actionable plan to prepare for and quickly adapt to the changing landscape of healthcare regulatory compliance:

1. Stay Informed, Monitor Regulatory Updates & Assess Impact on Current Tech Roadmap

Stay current on any regulatory changes by subscribing to updates from official sources such as the U.S. Department of Health and Human Services (HHS), Federal Register, and other relevant bodies that govern HIPAA. Proactively monitoring changes allows the organization to adjust before regulations are finalized or implemented. This proactive approach puts you in control of how you design and implement ongoing technology initiatives, especially if you are embarking on a significant transformation initiative around security, AI, cloud, data, or applications.

2. Conduct a HIPAA Compliance Gap Assessment in Line with NIST Frameworks

Conducting a HIPAA compliance assessment alongside supplemental security, risk, and privacy frameworks such as NIST is essential. This should focus on areas that might be impacted by the potential changes (e.g., data sharing, new privacy rules, or encryption standards, and AI systems). A thorough gap analysis helps identify where the current compliance efforts might fall short with respect to the potential regulatory changes. This would include a review of internal policies, procedures, and the technical safeguards in place for PHI and ePHI, providing early visibility of needed changes to comply with the updated rule set.

3. Review & Update Risk Management Practices

Evaluating and updating the organization's risk management framework to address both existing and emerging risks, particularly in the context of AI, cloud services, and third-party vendors (business associates), is crucial. If the changes to HIPAA introduce more stringent requirements for data security, risk assessments, or third-party oversight, the risk management process should be agile and capable of adapting to those changes.

4. Evaluate Data Protection Mechanisms for AI & Emerging Technologies

Given that HIPAA may evolve to address innovative technologies such as AI in healthcare, review the security measures in place for systems that utilize AI to process or analyze ePHI. This proactive approach would first require an inventory that identifies systems or applications that leverage AI. AI systems must be thoroughly assessed for their data protection controls including encryption, access controls, transparency, and vulnerabilities.

5. Review Vendor & Third-Party Relationships

Review and update contracts with third-party vendors and business associates to ensure they have business associate agreements (BAAs) and evaluate the proposed rule change to understand how the organization would establish new BAAs with existing entities as well as the magnitude of that effort. If HIPAA evolves to address new risks associated with data sharing, AI, or data breaches, the BAA language is likely to change, requiring established vendors and third parties to agree to updated terms.

6. Ensure Continuous Monitoring & Detection Systems Are Adapted

Ensure that security monitoring systems (e.g., SIEM, intrusion detection systems) are updated to detect AI-related threats or attacks, including adversarial AI and data breaches involving ePHI. If HIPAA evolves to reflect new threat vectors or stricter data protection requirements, continuous monitoring systems should be able to detect these specific threats, such as those targeting AI models or cloud storage systems.

7. Implement or Strengthen Incident Response Capabilities

Revise incident response plans to account for new potential threats, including those that might arise from AI-driven systems or new breach notification requirements under HIPAA. If new regulations expand the definition of a breach or the timeline for notification, incident response teams must be prepared to act swiftly and in compliance with those rules.

Given the potential introduction of more stringent controls or transparency requirements for AI in healthcare, update recovery plans to ensure that AI systems and ePHI can be restored in compliance with HIPAA regulations after a cybersecurity incident. AI systems may require specific validation before they are restored after a security breach, particularly when they involve ePHI. These systems need to be resilient, with quick recovery processes in place to maintain compliance. Isolated Recovery Environments should be established to protect organizations from threats like ransomware.

8. Plan & Prepare Resources

A regulatory change of this magnitude will come at a cost. Healthcare organizations should evaluate the proposed rule and build a plan that includes consideration for people, processes, and technology solutions that may be essential to achieve compliance. Be ahead of the curve.

The organizations that familiarize themselves with the rule, participate in the public comments period, and assess their environment to understand its impact are better positioned to reduce costs, as well as adverse operational and strategic effects of such tremendous change.

A proactive step for impacted organizations is to measure the current implemented standards against the NIST security frameworks as well as the existing HIPAA requirements to identify any gaps in their controls. As the new HIPAA iteration is released, the NIST analysis can be correlated to the new requirements to identify those areas where new remediation is required.

Contributing Authors:

Ranj Krishnamurthy, Senior Director, Solutions Development

Alan Grantham, VP, Security Consulting

Nina Wyatt, Director, Security

AHEAD

Contact AHEAD to learn how we partner with healthcare organizations to minimize adverse effects of regulatory change and strategically position clients for success.

Contact Us

National Hubs

CHICAGO

444 W. Lake Street
Suite 3000
Chicago, IL 60606

NEW YORK

500 Fifth Avenue
Suite 1700
New York, NY 10110

ATLANTA

1117 Perimeter Center
W406
Atlanta, GA 30338

SAN FRANCISCO

2000 Crow Canyon Place
Suite 250
San Ramon, CA 94583