COLORTOKENS

WHITEPAPER

HHS Focuses on Healthcare Cybersecurity with Proposed Rule Changes: What you Should Know

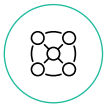
Background

On January 6, 2025, the U.S. Department of Health and Human Services Office for Civil Rights (OCR) issued a notice of proposed rulemaking (the "proposed rule"), which proposes several significant updates to the HIPAA Security Rule and the Health Information technology for Economic and Clinical Health Act of 2009 (HITECH Act). The comment period for the proposed rules ends on March 7th, 2025, and the rules are to be in effect in June 2025.

These proposed revisions to security rules are designed to address the increased risk to healthcare organizations from cyberattacks such as ransomware. The new rules aim to enhance cybersecurity measures for electronic Protected Health Information (ePHI) by:

Requiring encryption of sensitive medical data

The use of multi-factor authentication as a defense against phishing



Increasing network security controls, such as network segmentation

The Security Rule was initially published in 2003 and most recently revised in 2013. Since its publication, there have been significant changes to the environment in which health care is provided and how the health care industry operates, but the law has remained unchanged.

Almost every stage of modern health care relies on stable and secure computer and network technologies, including, but not limited to: appointment scheduling, prescription orders, telehealth visits, medical devices, patient records, medical and pharmacy claims submissions and billing, insurance coverage verifications, payroll, facilities access and management, internal and external communications, and clinician resources.

The proposals in this proposed rule would increase the cybersecurity for ePHI by revising the Security Rule to address:

1. Changes in the environment in which health care is provided.
2. Significant increases in breaches and cyberattacks.
3. Common deficiencies the Office for Civil Rights has observed in investigations into Security Rule compliance by covered entities and their business associates (collectively, ‘‘regulated entities’’).
4. Other cybersecurity guidelines, best practices, methodologies, procedures, and processes; and Court decisions that affect the enforcement of the Security Rule.

Applicability

The effective date of the final rule would be 60 days after publication. Regulated entities would have until the “compliance date” to establish and implement policies, procedures, and practices to achieve compliance with any new or modified standards.

Most of the proposed modifications would provide regulated entities with greater clarity and specificity on fulfilling their obligations and the Department’s expectations. Accordingly, we do not believe the proposed rule would pose unique implementation challenges that would justify an extended compliance period (i.e., a period longer than the standard 180 days provided in 45 CFR 160.105.

By design, the Security Rule sets a national floor for the security measures that regulated entities are required to implement to protect the confidentiality, integrity, and availability of ePHI.

Summary of Key Changes in the Proposed Rules

1. **Changes to the definition of "Electronic Media" under the HIPAA Security Rule**

The Department proposes revisions to the definition of "electronic media" to reflect technological advancements and address evolving methods of storing, transmitting, and processing electronic protected health information (ePHI). Implications: The updated definition aims to modernize the Security Rule by incorporating advancements in electronic communication and storage, addressing vulnerabilities, and preparing for future innovations in health information technology. These changes are expected to enhance the cybersecurity of ePHI and provide clearer guidelines for regulated entities.

2. **Mandating the creation and maintenance of a written inventory of technology assets and a network map.**

Regulated entities will need to review and update their asset inventory and network map on an ongoing basis, but at least once every 12 months and when there is a change in the environment or operations that may affect electronic protected health information (ePHI).

3. **Removal of the Distinction Between "Addressable" and "Required" Implementation Specifications**

For background, the Security Rule contains specific administrative, physical, technical, organizational, and documentation standards and associated implementation specifications. The current Security Rule contains both "required" and "addressable" implementation specifications. Required specifications must be implemented. Addressable specifications require that the covered entity or business associate (either, a "regulated entity") assess whether the specification is reasonable and appropriate in the regulated entity's environment regarding the likely contribution to protecting electronic protected health information (ePHI) and, if the specification is not reasonable and appropriate, document why and implement an equivalent alternative measure that is reasonable and appropriate.

The proposed rule would remove the distinction between "required" and "addressable" implementation specifications and require all implementation specifications, except in limited circumstances. In the preamble, OCR states that it is concerned that some regulated entities misunderstand "addressable" specifications to be optional. While the preamble emphasizes that the proposed rule aims to maintain flexibility in the Security Rule, the removal of this distinction is meant to clarify that **implementation of the specifications is not optional; a regulated entity must implement the standards and associated specifications and adopt reasonable and appropriate security measures to achieve such implementation.**

4. Greater Specificity for Risk Analyses

While the current Security Rule requires that a regulated entity conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the regulated entity, the proposed rule would impose more specific requirements for such risk analyses. In particular, the proposed rule would require a written assessment that documents details related to eight specifications, including:

a. Review of the regulated entity's technology asset inventory and network map.

b. Identification of all reasonably anticipated threats to the confidentiality, integrity, and availability of ePHI.

c. Identification of potential vulnerabilities and predisposing conditions to the regulated entity's relevant electronic information systems.

d. Determination of the potential impact of each identified threat, among other requirements.

The preamble states that these requirements for risk analyses would be distinct from the evaluation standard, which requires a regulated entity to proactively consider whether risks or vulnerabilities will be introduced by any changes to the regulated entity's environment or operations.

5. Incident and Disaster Response Requirements

The proposed rule would require that a regulated entity establish a security incident response plan and implement procedures for testing and revising those plans at least once every 12 months. A regulated entity would also be required to develop and maintain documentation of investigations, analyses, mitigation, and remediation for suspected or known security incidents. Further, a regulated entity would be required to have contingency plans in place, including procedures to restore its critical electronic information systems and data within 72 hours of a loss and restore other systems and data in accordance with the criticality analysis contained in the regulated entity's written contingency plan. A business associate would be required to notify covered entities (or a subcontractor business associate to notify business associates) upon activation of their contingency plans without unreasonable delay, but in no later than 24 hours after activation.

4. Verification of Business Associates' Technical Safeguards.

The proposed rule would require that a regulated entity verify that an entity that creates, receives, maintains, or transmits PHI on its behalf is in fact taking necessary steps to protect ePHI. In particular, the proposed rule would require that a covered entity obtain a written verification, at least once every 12 months that a business associate has deployed technical safeguards required by the Security Rule, including a written analysis of the business associate's relevant electronic information systems. The same requirement would apply to business associates with respect to their subcontractor business associates.

5. Patch Management

The proposed rule would include a new standard for patch management, which would require that a regulated entity implement policies and procedures to identify, prioritize, and apply software patches throughout its electronic information systems that create, receive, maintain, or transmit ePHI or otherwise affect the confidentiality, integrity, or availability of ePHI. The proposed rule would impose specific timing requirements for patching, updating, or upgrading the relevant electronic information system: (i) 15 calendar days for a critical risk patch; (ii) 30 calendar days for a high-risk patch; and (iii) a reasonable and appropriate period of time-based on the entity's policies and procedures for all other patches.

6. Strengthened Access Control Requirements

The proposed rule would require that a regulated entity implement written policies and procedures related to its workforce member's access to ePHI and relevant electronic information systems, including termination of such access where appropriate, such as upon termination or a change in an employee's role. The proposed rule would also require that a regulated entity notify other regulated entities after a change in or termination of a workforce member's authorization to access ePHI of those other regulated entities as soon as possible but no later than 24 hours after the change or termination.

7. Compliance Audits

The proposed rule would require a regulated entity to perform and document an audit of its compliance with each standard and implementation specification of the Security Rule at least once every 12 months.

8. Documentation Requirements

The proposed rule would require that a regulated entity document in writing all policies, procedures, plans, and analyses required by the Security Rule, and review that documentation at least annually and in response to changes in its security environment or operations. This would include (but not be limited to) the requirements related to the technology asset inventory, network map, and risk analysis discussed above.

9. Workforce Sanctions

The proposed rule would include additional specifications related to the sanctioning of workforce members who fail to comply with a regulated entity's security policies and procedures, including the requirement to establish and maintain written policies and procedures related to workforce sanctions and document instances of and the circumstances leading to a regulated entity imposing sanctions on a workforce member.

10. Additional Security Measures

The proposed rule would require several additional security controls, each with limited exceptions, related to:

- **e.** Encryption of ePHI at rest and in transit;
- **f.** Multi-factor authentication;
- **g.** Network segmentation;
- **h.** Vulnerability scanning at least once every six months and penetration testing at least once every 12 months;
- **i.** Deployment of anti-malware protection;
- **j.** Removal of extraneous software from electronic information systems;
- **k.** disablement of network ports in accordance with a regulated entity's risk analysis; and
- **l.** Backup and recovery of ePHI.

Implications for Regulated Entities

The proposed rule increases the compliance burden on regulated entities, requiring more stringent risk management, technology oversight, and third-party security validation. Organizations must proactively review their security programs, strengthen cybersecurity measures, and enhance documentation practices to align with these new requirements. While the rule aims to provide greater security, it also necessitates significant operational and administrative adjustments.

Mapping HIPAA Security Rule Requirements to ColorTokens' Solution Capabilities

ColorTokens offers **Zero Trust**-based cybersecurity solutions that align with the proposed HIPAA Security Rule updates in the area of **network segmentation, asset inventory, risk analysis, vulnerability scanning, and disablement of risky network ports.**

ColorTokens' **Xshield Enterprise Microsegmentation Platform** enables providers to meet existing regulations and these new proposed rules with an easy to deploy technology solution. Installation takes mere hours, even in very large hospital environments, and the implementation of Xshield's Zero Trust enforcement is non-disruptive and will achieve a significant improvement in your healthcare system's security posture in 90 days or less.

Below is a direct mapping of HIPAA requirements for ColorTokens' solutions:

1. Network Segmentation

HIPAA Requirement:

- Regulated entities must implement **network segmentation** to isolate ePHI and prevent unauthorized lateral movement.
- Segmentation helps contain breaches, restrict access, and enhance compliance with access control policies.

ColorTokens Solution Capabilities to Address This Requirement

- ColorTokens' **Xshield Enterprise Microsegmentation Platform** enforces **Zero Trust segmentation** by isolating workloads, applications, and devices handling ePHI.
- Prevents the lateral movement of ransomware and malware in the event of a breach.
- Implements **software-defined microsegmentation** to create secure zones around ePHI environments.
- **Endpoint and network segmentation** to limit exposure of sensitive data.

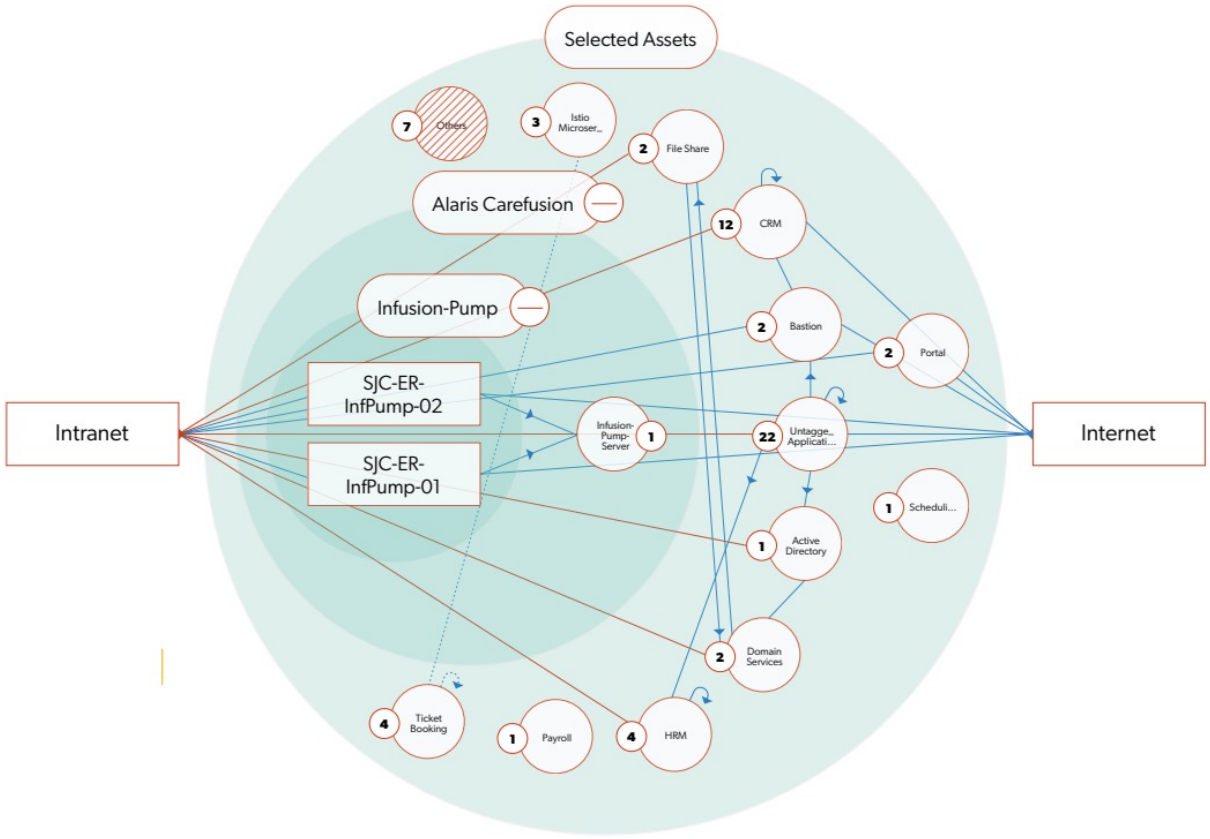
2. Technology Asset Inventory & Network Mapping

HIPAA Requirement:

- Entities must maintain an **updated asset inventory and network map** to track all ePHI-related systems.
- Continuous monitoring of devices and their interactions is required for compliance.

ColorTokens Solution Capabilities to Address This Requirement

- As shown in the figure below, The **Xshield Visualizer** shows all network resources and traffic, satisfying the requirement to provide **real-time visibility** into all assets interacting with ePHI.



- Generates an **interactive network map** that shows ePHI data flows and segmentation policies.
- dentifies all network traffic with color-coded lines indicating in-policy and out-of-policy communications
- Identifies **unprotected endpoints and workloads,** reducing security blind spots.

3. Risk Analysis & Vulnerability Management

HIPAA Requirement:

- Conduct thorough risk assessments that document security vulnerabilities in ePHI environments.
- Regularly scan for **threats, vulnerabilities, and unauthorized system interactions**.

ColorTokens Solution Capabilities to Address This Requirement

- **Vulnerability scanner** identifies misconfigurations and unauthorized access points.
- Maps **vulnerabilities in real-time**, helping organizations mitigate risks before they impact ePHI.
- Monitors in-policy and out-of-policy network interactions
- Provides **compliance reports** tailored to HIPAA requirements, ensuring readiness for audits.

4. Incident & Disaster Response Enhancements

HIPAA Requirement:

- Regulated entities must implement **incident response plans** and document security events.
- Organizations must restore critical systems **within 72 hours** after an incident.

ColorTokens Solution Capabilities to Address This Requirement

- **Automates threat containment** by quarantining compromised systems in real-time.
- Provides **forensic analysis of security incidents**, helping teams respond faster to breaches.
- **Ensures rapid recovery** by securing workloads and maintaining operations even during an attack.

5. Disable Network Ports in Accordance with Risk

HIPAA Requirement:

- Under the proposed implementation specification for network ports at proposed 45 CFR 164.312(c)(2)(iv), a regulated entity would be required to **disable network ports** in accordance with the regulated entity's risk analysis.
- Successful ransomware deployment often depends on exploiting technical vulnerabilities such as unsecured ports.
- The proposal to require network ports to be disabled in accordance with the risk analysis would reduce exploitable vulnerabilities.

ColorTokens Solution Capabilities to Address This Requirement

- Xshield automates the enforcement of controls on communications using known **risky protocols and ports**
- **Attack surface reduction** by disabling risky or unused network ports for enhanced endpoint security.

6. Annual Compliance Audits & Documentation Requirements

HIPAA Requirement:

- Regulated entities must perform **annual security audits** and document all security practices.
- Organizations must **review security policies, risk assessments, and technology usage annually.**

ColorTokens Solution Capabilities to Address This Requirement

- Provides **real-time compliance tracking** against HIPAA Security Rule standards.
- Generates detailed **audit reports** for security incidents, risk assessments, and access logs.
- Enables **continuous compliance monitoring**, ensuring organizations remain HIPAA-compliant year-round.

7. Workforce Sanctions & Security Training

HIPAA Requirement:

- Organizations must **enforce workforce security policies** and document non-compliance cases.
- Employees should receive **ongoing cybersecurity training**.

ColorTokens Solution Capabilities to Address This Requirement

- Tracks **anomalous network activity** and alerts security teams to sanctionable workforce behavior or intentional insider threats.
- Supports **Zero Trust security awareness programs** through continuous policy-based communications controls.

Conclusion: Why ColorTokens for HIPAA Compliance?

The proposed HIPAA Security Rule updates demand **enhanced cybersecurity, stronger compliance enforcement, and proactive risk management**. ColorTokens' **Zero Trust security solutions** directly align with these requirements by:

1. Implementing network microsegmentation to protect ePHI.

   Provides real-time visibility of assets inventory and network map
2. Executing vulnerability scanning and risk assessment.
3. Enhancing Incident & Disaster Response by quarantining compromised assets
4. Disabling Network Ports in Accordance with Risk
5. Satisfying annual compliance documentation requirements
6. Enforcing workforce security best practices by monitoring anomalous network activity

With **ColorTokens**, healthcare organizations can effectively secure ePHI, comply with HIPAA requirements, and safeguard patient data from cyber threats.

For more information: Breach Readiness for Hospitals & Healthcare Providers - ColorTokens

Sources:

https://www.cov.com/en/news-and-insights/insights/2025/01/hhs-issues-notice-of-proposed-rulemaking-to-update-the-hipaa-security-rule

https://www.insideprivacy.com/health-privacy/hhs-issues-notice-of-proposed-rulemaking-to-update-the-hipaa-security-rule/

https://www.hhs.gov/hipaa/for-professionals/security/hipaa-security-rule-nprm/factsheet/index.html

About ColorTokens:

ColorTokens is a leading provider of enterprise microsegmentation and breach containment solutions, dedicated to making organizations “breach ready.” By preventing the lateral spread of ransomware and advanced malware, ColorTokens protects complex network infrastructures through its innovative Xshield™ platform. The platform visualizes traffic between workloads, OT/IoT/IoMT devices, and users, enabling the enforcement of granular micro-perimeters, swift isolation of critical assets, and effective breach response. Recognized as a Leader in the Forrester Wave™: Microsegmentation Solutions (Q3 2024), ColorTokens delivers proactive security that prevents disruptions and safeguards global enterprises. For more information, visit www.colortokens.com.