# Proposed HIPAA 2025 Security Rule Impacts for Healthcare Entities

On January 6, 2025, the Department of Health and Human Services (HHS) issued a Notice of Proposed Rulemaking (NPRM) outlining modifications to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act). The proposed update affects all Covered Entities and Business Associates (Regulated Entities) regardless of size by adding new controls and making all controls mandatory.

The Security Rule update represents a significant overhaul of the cybersecurity requirements for HIPAA-regulated entities. The new Security Rule includes many requirements that align with current cybersecurity best practices, methodologies, and procedures and aims to improve protection of electronic protected health information (ePHI) against internal and external threats. It also includes changes responding to court decisions that have affected how the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) enforces the HIPAA Security Rule.

## Evolving Cybersecurity Challenges in Healthcare

### 1 Regulatory compliance

Urgency for payers, providers and business associates to comply with HIPAA and Office for Civil Rights (OCR) requirements leveraging NIST cybersecurity frameworks. Compliance will change even more once the Security Rule is finalized.

### 2 Expanded third-party threat attack surfaces

A high dependency on suppliers, contractors and joint ventures increases exposure to supply chain attacks, firmware tampering and insecure vendor connections.

### 3 AI-driven cyberattacks

AI agents capable of planning and executing complex tasks are being weaponized to hijack systems and steal data. According to Forbes, 87% of security professionals have encountered AI-driven cyberattacks.

### 4 Digital transformation in payor systems

Digital technologies such as GenAI, Large Language Model development, robotic automations, and telehealth streamline patient interactions and improve patient health but they introduce new vulnerabilities that require robust governance and ethical AI frameworks.

### 5 OT/IT interdependencies

The intersection of OT/IoT and IT technologies increases complexity and threat exposure, expands the attack surface and complicates patch management and asset visibility.

### 6 Security risks from legacy systems and limited cloud adoption

Outdated technologies designed to support on-premises systems may not be compatible with cloud architectures, such as SAAS, PAAS or IAAS. Multi-tenant environments are incompatible with modern security technologies.

### 7 Medical device vulnerabilities

Threats targeting connected medical devices (e.g., glucose monitors) are increasing due to their integration with patient data systems.

### 8 Ransomware and DDoS escalation

Healthcare ransomware and DDoS attacks are on the rise due to their critical data and operational urgency.

### 9 Cybersecurity maturity gaps

Limited visibility of ROI on security investments and challenges in aligning cyber programs with business goals makes it difficult to assess and improve cybersecurity maturity.

## Key changes in the proposed Security Rule

Historically, the Security Rule includes standards and specifications for implementing those standards. These implementation standards are currently categorized as "required" or "addressable." Regulated entities have discretion in determining if addressable controls are reasonable and appropriate following a documented risk analysis. The proposed changes remove the addressable designation so all implementation specifications will now be required.

HHS has defined specific controls and requirements to further strengthen ePHI security, including:

- Enhanced data governance — New requirements for identifying, classifying, and protecting ePHI
- Incident detection — Stricter requirements for incident detection and log maintenance
- Regular testing and evaluation — Regular testing of access controls and securing privileged access management, including retesting after a significant introduction or change in technology, application design or underlying systems
- Network segmentation — Segmentation of operational and IT networks, including EHR, medical devices, and financial systems
- Expanded identity requirements — Inclusion of assets, software, and automation (AI, RPA, BOTS) in identity definitions as well as access termination to all ePHI applications within one hour of a breach detection
- Patch and vulnerability management — Six implementation specifications with a 15-day patch requirement from vendor release
- Multi-Factor Authentication — Required for systems accessing ePHI
- RTO within 72 hours — Written procedures to restore critical information systems within 72 hours and requirements for underlying data to be no more than 48 hours old from the time of a breach
- Asset map and data flows — Maintenance of written technology asset inventories, network mapping, and integrated ePHI data flows
- Risk analysis — Eight implementation standards for annual risk analysis and compliance auditing, including changes in ePHI environments

If enacted, the Security Rule changes will have significant impacts on HIPAA-regulated entities both from a financial and operational standpoint and may require major cybersecurity investments.

## How Wipro can help

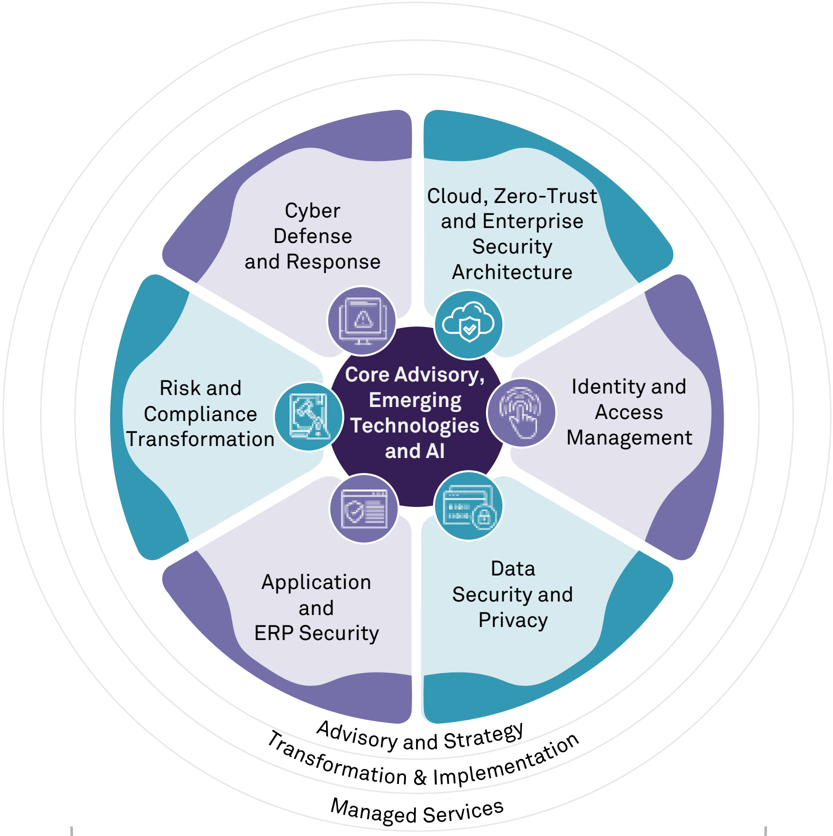
Wipro's global practice leaders are experienced in working with relevant government and federal directives. Our integrated cybersecurity and risk advisory approach spans risk and compliance, cyber assurance, privacy, cloud security, applications security, data protection models and cyber defense. Wipro can help organizations achieve end-to-end HIPAA compliance through solutions and services that offer:

- HIPAA compliance reviews and analysis
- Business associate compliance and enhanced third-party risk management
- Identity management for people, technology, and assets
- Data governance to improve ePHI management
- Vulnerability/patch risk management programs with enhanced AI
- Network segmentation and asset risk strategies.
- Business continuity and disaster recovery (BCDR) services to ensure 72-hour RTO compliance
- Incident response services to meet 24-hour notification requirements
- Information Security Officer services to help maintain HIPAA documentation, including asset inventories, ePHI data flows, control implementations, and results of security testing and remediation

## Life Sciences and Medical Device Challenges

- Expanded Identity Requirements
- Frequent Patch, Vulnerability, Logging and Detection
- Network Security
- Enhanced Data Governance
- Asset Mapping and Data flow
- Risk Analysis and Compliance Auditing
- Business Continuity and Disaster Recovery
- Regular Testing and Evaluation

## Wipro's offerings in alignment with Life Sciences and Medical devices challenges and HIPAA changes



Core Advisory, Emerging Technologies and AI

Cyber Defense and Response

Cloud, Zero-Trust and Enterprise Security Architecture

Identity and Access Management

Data Security and Privacy

Application and ERP Security

Risk and Compliance Transformation

Advisory and Strategy

Transformation & Implementation

Managed Services

### HIPAA Changes

**IAM**
- MFA Access for ePHI
- Deprovisioning - 1 hr. after termination
- Auditing PAM
- Identity for Tools, Assets and Software

**Threat & Vulnerability Management**
- Patch within 15 days
- Enhanced logging and detection

**Data Security**
- ePHI encrypted at rest and transit
- Asset mapping and Data Flows
- BCP / DR within 72 hours
- Data classification per global privacy regulation

**Governance, Risk & Compliance (GRC)**
- Annual Risk Analysis and Compliance Auditing

**Network Security**
- Network Segmentation across IT, Ops, EHR, Finance

**AI Security**
- AI, Bots, RPA are now part of Identity
- AI in Security operations
- AI in Data transformations and Analytics

Wipro's comprehensive suite of partnerships, acquisitions and venture investments empower us to strategize, advise, standardize, re-engineer and govern aspects of cybersecurity using a risk-based approach. By leveraging Wipro's expertise, organizations can navigate the complexities of HIPAA 2025 and ensure robust compliance with the new regulations.

**Sources:**

HIPAA Security Rule Notice of Proposed Rulemaking (NPRM) – Fact Sheet

HIPAA Security Rule NPRM – Full Rulemaking Text

Federalregister.gov/d/2024-30983/p-292

Federalregister.gov/d/2024-30983/p-300

Federalregister.gov/d/2024-30983/p-304

Federalregister.gov/d/2024-30983/p-306

**Wipro Limited**
Doddakannelli
Sarjapur Road
Bengaluru – 560 035
India

Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
**wipro.com**

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading technology services and consulting company focused on building innovative solutions that address clients' most complex digital transformation needs.

Leveraging our holistic portfolio of capabilities in consulting, design, engineering, and operations, we help clients realize their boldest ambitions and build future-ready, sustainable businesses. With over 230,000 employees and business partners across 65 countries, we deliver on the promise of helping our clients, colleagues, and communities thrive in an ever-changing world.

For additional information, visit us at **www.wipro.com**