Understanding the New HIPAA HIPAA Security Rule on Cybersecurity

Key Changes and Implications for Medical Providers - March 2025

Heath Morgan
General Counsel
BC Services, Inc.

Heath Morgan

Heath is General Counsel for BC Services, and has over 20 years in the revenue cycle management Industry. He is passionate about education through many mediums, and has presented on many aspects of the Revenue Cycle industry for the Arkansas, Colorado, Hawaii, Louisiana, Oklahoma, and Texas Chapters of HFMA, HFMA Region 9, the Oklahoma Hospital Association (OHA), the Medical, Dental, and Hospital Business Association (MDHBA), and the Rocky Mountain American Association of Healthcare Administrative Management (AAHAM).

Heath is the author of a science fiction novel on the future of AI technology and what it means for our world called “The Memory Project”.

Rule Timeline

Publication Date

January 6, 2025

Comment Period

Ended March 7, 2025

Implementation Timeline

Variable, Expected Summer 2025

HIPAA Updates: Why Now?

Overview of HIPAA

Protecting patient information

Proposed Updates

Brief mention of Security Rule changes

Rising Cyber Threats

Healthcare targeted

Driving Forces Behind the HIPAA Security Rule Update

1. **Increase in Cyber Threats**

   Targeting healthcare organizations

2. **Need for Stronger Protections**

   For electronic protected health information (ePHI)

Key Changes to the Security Rule

1. Eliminate Addressable Specifications
2. Enhanced Risk Analysis
3. Mandatory Measures

Mandatory Security Measures Measures

Encryption

ePHI at rest and in transit

Multi-Factor Authentication Authentication

Accessing sensitive data

Elevated Risk Analysis

1. Comprehensive Risk Assessments
2. Technology Asset Inventory
3. Network Maps

AI Technology

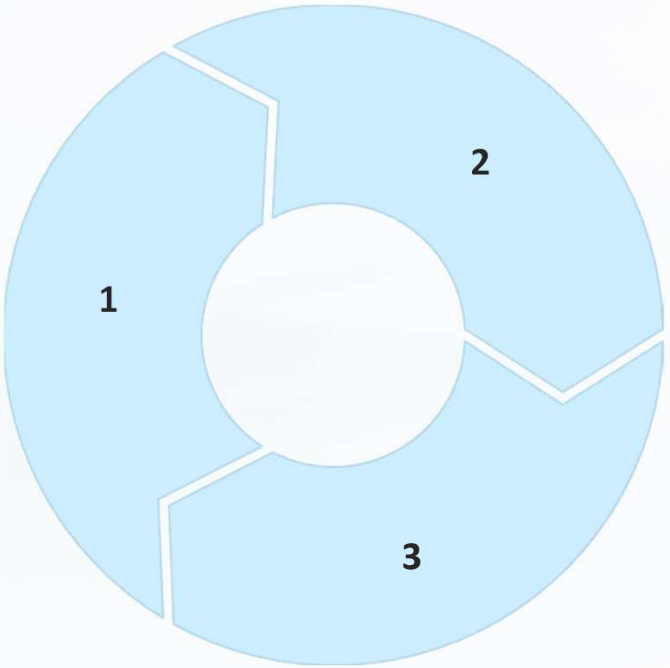
The proposed HIPAA Security Rule addresses the use of AI in healthcare contexts and its implications for ePHI protection.

The proposed regulations acknowledge that AI technology can involve:

1. **AI training data**
2. **Algorithm data**
3. **Prediction models**

If a covered entity's AI model uses patients' or participants' data, there could be potential unauthorized uses and disclosures of ePHI. As such, covered entities using AI tools would be required to include these tools in their risk analysis and risk management compliance activities.

Staying Compliant: Audits & Oversight



Annual Internal Audits

Business Associate Oversight

Patch Management

Proactive Measures to Prepare for Compliance

Let’s Take an Honest Look at Business Associates, Vendors, and Data in the Age of AI

- You are using AI technology already through intentional Vendors and unintentional vendors
- We Are Past the Stage Where You Can Outright Ban or Prohibit AI Use for Vendors in Contracts
- Contract Language Addressing AI, Algorithms, Data Are Out Dated, Obsolete, and Send Mixed Messages to Your Vendors
- This Can Lead to You or Your Vendor Being Out of Compliance with the Contract Language for Oversight Purposes, and if Something Goes Wrong that involves AI, you don’t really know what happened.
- This Technology is Moving Too Fast to Be Locked into One Sentence

Let’s Take an Honest Look at Business Associates, Vendors, and Data in the Age of AI

- Resetting the AI Conversation with Vendors starts with Conversations with Your Provider Legal Department
- Create a Vendor AI Survey to Collect All Use Cases and that they are currently using, using with other Providers, and want to use in the Future
  - How Do We Want AI to Be Used?
  - What AI Use Are We Ok With?
  - Work From Home, Cars, Zoom/Teams Calls, Iphone IOS 18, Smart Devices

Let’s Take an Honest Look at Business Associates, Vendors, and Data in the Age of AI

- Create a Vendor Addendum that Address AI
  - Addresses: Gen AI, Conversational AI, Machine Learning, and Automation
  - Addresses Data: Regulatory Protected Data, Non Regulatory Protected Data
  - Addendum Should Set Regular Meetings with Vendors to Discuss AI Developments & Risk Assessments & Use Cases (Monthly, Quarterly, Bi-annually)

HIPAA Security Rule: Timeline

1

March 7, 2025

Comment Period Ends

2

Final Rule Adoption

3

Grace Period

Anticipated Timeline for Final Rule Adoption

Estimated Costs of Compliance

1. Mid-range estimates for HIPAA compliance: $80,000 to $120,000 per organization
2. Annual maintenance costs for health information technology:
   Around $35,000 per physician
3. Costs vary based on organization size, nature, and existing compliance level

Financial Considerations

- Investments required for:
  - Updated technologies and processes
  - Multi-factor authentication implementation
  - Advanced encryption protocols
  - Additional IT staff or consultants
  - Updated training programs
  - Regular security assessments and audits
- Potential for reduced costs from fewer data breaches
- Financial assistance may be available through grants or program

Questions?

Heath Morgan

heath.morgan@bcservice.com