EPSTEIN BECKER GREEN

HIPAA, HISAA, and More:
Evolving Data Security Rules for Hospitals

Allen Killworth **Lisa Pierce Reisz**

Ohio Hospital Association Annual Meeting

May 19, 2025

Agenda

- Introduction
- HISAA Proposed Statute (died on Jan. 3, 2025)
- HIPAA Proposed Rule
- CIRCIA Proposed Rule
- Questions

EPSTEIN
BECKER
GREEN

HISAA

Health Infrastructure Security and Accountability Act

HISAA Background

- Introduced (S.5218) by Senators Ron Wyden (D-OR) and Mark Warner (D-VA) in September 2024 in response to high-profile cyberattacks on hospitals.
- Senator Wyden: “Megacorporations like UnitedHealth are flunking Cybersecurity 101, and American families are suffering as a result … The health care industry has some of the worst cybersecurity practices in the nation despite its critical importance to Americans’ well-being and privacy.”
- Summary document of proposed law stated:

  According to the FBI, the health care sector is now the #1 target of ransomware. These hacks are entirely preventable and are the direct result of lax cybersecurity practices by health care providers and their business partners. Cybersecurity failures have delayed and disrupted patient care, and have harmed patient health and privacy, as well as national security. Despite these high stakes, health care has some of the weakest cybersecurity rules of any federally regulated industry.

HISAA: Security Requirements

- HISAA would require HHS to develop two sets of new regulations:
  - **Minimum security requirements** for all HIPAA Covered Entities and Business Associates. The minimum security requirements are to be designed to prevent cyber incidents and harms to Covered Entities, Business Associates, and patients resulting from cyber incidents.
    - ➢ HHS would be required to review and update the minimum security requirements and enhanced security requirements at least every two years.
  - **Enhanced security requirements** for those HIPAA Covered Entities and Business Associates determined by HHS to be of systematic importance to national security. The enhanced security requirements are to be designed to protect against the specific threats faced by those Covered Entities and Business Associates which are of systematic importance to national security.

HISAA: Risk Assessments, Audits, and Reports

- CEs and BAs would be required to conduct a cybersecurity risk assessment annually, to include:
  - Documenting a plan for rapid and orderly resolution in the event of natural disaster, disruptive cyber incident, or other technological failure to its information systems;
  - Conducting a stress test to evaluate whether the entity has the capabilities and planning necessary to recover essential functions following a cyber incident, natural disaster, or other threat to operations;
  - Documenting revisions to prior plans produced in the annual assessments; and
  - Written statement from CEO and CISO that the entity is in compliance with the security requirements.
- CEs and BAs would be required to contract with an independent auditor to conduct an annual audit to: (1) assess the compliance with the minimum/enhanced security requirements and Cybersecurity Performance Goals to be established by HHS; (2) identify areas where requirements not met; and (3) certify that the entity has resolved noncompliance or is implementing an appropriate plan to resolve the noncompliance.
- CEs and BAs subject to enhanced security requirements would be required to report both the risk assessment and audit information to HHS annually, and other entities to report as required by HHS.
- HHS would be required to conduct an audit of at least 20 CEs or BAs annually.

HISAA: Penalties & Fees

- HISAA would establish tiered civil monetary penalties for failure to comply with the new minimum security requirements and enhanced security requirements. Unlike current civil monetary penalties for HIPAA violations, these penalties would **not** be subject to the statutory maximum limit.
- HISAA would establish civil monetary penalties of up to $5,000 per day for failure to comply with the new risk assessment, audit, and reporting requirements as well as criminal penalties for reporting false information.
- HHS would be authorized to charge fees to CEs and BAs to cover the costs of oversight and enforcement of these activities (total fees could not exceed $40 million in fiscal year in 2026, $50 million in 2027, and amounts increasing based on the consumer price index in later years).

HISAA: Medicare Assistance

- HISAA would provide $800 million to go to critical access hospitals and eligible high-needs hospitals to assist with adoption of cybersecurity practices.
- An additional $500 million would be made available to all hospitals to incentivize adoption of cybersecurity practices. Hospitals would be subject to payment reductions for failing to adopt enhanced cybersecurity practices.
- HISAA would codify the authority of HHS to provide Medicare payments to providers that have significant cash flow problems resulting from unusual circumstances including disruption of claims processing due to a cybersecurity incident.

EPSTEIN
BECKER
GREEN

HIPAA
Proposed Security Rule

Overview

- On December 27, 2024, OCR announced a Notice of Proposed Rulemaking (NPRM): HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information (published January 6, 2025).
- Then-Director of OCR Melanie Fontes Rainer:

  > Cyberattacks continue to impact the health care sector, with rampant escalation in ransomware and hacking causing significant increases in the number of large breaches reported to OCR annually. The number of people affected every year has skyrocketed exponentially, a number we expect to grow even bigger this year with the Change Healthcare breach, the largest breach in our health care system in U.S. history. … This proposed rule to upgrade the HIPAA Security Rule addresses current and future cybersecurity threats. It would require updates to existing cybersecurity safeguards to reflect advances in technology and cybersecurity, and help ensure that doctors, health plans, and others providing health care meet their obligations to protect the security of individuals' protected health information across the nation.

- First update to HIPAA Security Rule since 2013.

New, But Not New…

- Many of the substantive requirements in the Proposed Rule are already incorporated in various guidelines and safeguards for protecting sensitive information, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework and HHS's cybersecurity performance goals (CPGs).
- Voluntary compliance with these recognized guidelines has been incentivized pursuant to the HITECH Act's 2021 amendment because a CE/BA that adopts "recognized security practices" is entitled to have its adoption considered by OCR in determining fines and other consequences.
- Moreover Ohio (like many states) provides a safe harbor to some state law data breach claims if the entity has adopted a qualifying cybersecurity program, which must confirm to certain programs including the NIST Framework for Improving Critical Infrastructure Cybersecurity or comply with HIPAA cybersecurity requirements (ORC 1354.01–.05).

Key Provisions

- New/Updated Definitions
  - 15 revised definitions and 10 new definitions, including new key terms such as "risk," "threat," and "vulnerability."
  - Updates to definition of "information systems" and new definitions of "electronic information system" and "relevant electronic information system." Proposed makes distinctions when **all** electronic information systems must abide by a rule versus only the **relevant** electronic information systems.
  - Definition of "relevant electronic information systems" include electronic information systems that create, receive, maintain, or transmit ePHI **or that otherwise affect the confidentiality, integrity, or availability of ePHI**. Would include electronic systems that do not contain any ePHI but may affect access to and/or the confidentiality or integrity of ePHI.
- Addressable vs. Required
  - Current Security Rule categorizes implementation specifications as either "addressable" (i.e., which give Regulated Entities flexibility in how to approach them) or "required" (i.e., they must be implemented by Regulated Entities). OCR noted that it has become concerned that CEs/BAs view addressable implementation specifications as optional, thereby reducing the ultimate effectiveness of the Security Rule.
  - Proposed Rule would remove the distinction between "addressable" and "required" specifications, making **all** implementation specifications required, except for a few narrow exemptions.

Key Provisions

- Changes to Risk Analysis
  - Proposed Rule would impose specific requirements that must be included in a risk analysis and its documentation, including:
    - a review of the aforementioned technology asset inventory and network map;
    - identification of all reasonably anticipated threats to the ePHI created, received, maintained, or transmitted;
    - identification of potential vulnerabilities to the relevant electronic information systems;
    - an assessment and documentation of the security measures used to ensure that the measures protect the confidentiality, integrity, and availability of the ePHI;
    - a reasonable determination of the likelihood that "each" of the identified threats will exploit the identified vulnerabilities; and
    - if applicable, a reasonable determination of the potential impact of such exploitation and the risk level of each threat.
  - Proposed Rule would require that risk analyses be reviewed, verified, and updated at least once every 12 months or in response to environmental or operational changes impacting ePHI.
  - In addition to the risk analysis, Proposed Rule would require CEs/BAs to create a written evaluation to determine whether any and all proposed changes in environment or operations would affect the confidentiality, integrity, or availability of ePHI prior to making that change.

Key Provisions

- Technology Asset Inventories & Network Maps
  - Current Security Rule requires assessment of threats, vulnerabilities, and risks but stops short of prescribing particular methods or means of doing so.
  - Proposed Rule would imposed explicit requirements to create a technology asset inventory and a network map.
    - The technology asset inventory would require written documentation identifying all technology assets, including location, the person accountable for such assets, and the version of each asset.
    - The network map must illustrate the movement of ePHI through electronic information systems, including how ePHI enters, exits, and is accessed from outside systems. Additionally, the network map must account for the technology assets used by business associates to create, receive, maintain, or transmit ePHI.
    - Both the technology asset inventory and network map would need to be reviewed and updated at least once every 12 months.
- Verifying BA Compliance
  - Proposed Rule would require verification of BA technical safeguards.
  - CEs must obtain written verification of the technical safeguards used by BAs that create, maintain, or transmit ePHI on their behalf at least every 12 months. Such verification must be written by a person with appropriate knowledge of, and experience with, generally accepted cybersecurity principles and methods.

Key Provisions

- Patch Management
  - Proposed Rule would create a new patch management standard requiring CEs/BAs to implement policies and procedures for identifying, prioritizing, and applying software patches throughout their relevant electronic information systems, including specific timing requirements based on the criticality of the patch in question:
    - 15 calendar days for a critical risk patch,
    - 30 calendar days for a high-risk patch, and
    - a reasonable and appropriate period of time for all other patches.
- Workforce Controls
  - OCR expressed concern with compliance with current Security Rule general workforce management requirements
  - Proposed Rule would establish more explicit requirements for workforce control policies, which must be written and reviewed at least once every 12 months.
  - In addition, the Proposed Rule would impose strict timing requirements for workforce access and training:
    - Terminated employees' access to systems must end no later than one hour after termination.
    - Other CEs/BAs must be notified after a change in or termination of a workforce member's authorization to access ePHI of those entities no later than 24 hours after the change or termination.
    - New employees must receive training within 30 days of establishing access and at least once every 12 months thereafter.

Key Provisions

- Technical Safeguards
  - Proposed Rule would require CEs/BAs to use multi-factor authentication requirements that are consistent with the CPGs. Multi-factor authentication would require verification through at least two of the following categories:
    - Information known by the user, such as a password or personal identification number (PIN);
    - Items possessed by the user, including a token or a smart identification card; and
    - Personal characteristics of the user, such as a fingerprint, facial recognition, gait, typing cadence, or other biometric or behavioral characteristics.
  - Other Minimum Technical Safeguards
    - minimum password strength requirements that are consistent with NIST
    - segregation of roles by increased privileges
    - automatic logoff
    - log-in attempt controls
    - network segmentation
    - encryption at rest and in transit,
    - anti-malware protection
    - standard configuration for OS and software
    - disable network ports
    - audit trails and logging
    - vulnerability scanning every six months
    - penetration testing every 12 months

Key Provisions

- Contingency/Disaster Planning
  - Proposed Rule would add obligations relative to contingency planning, including requirements to identify critical electronic information systems.
  - Proposed Rule would establish relatively short timing requirements:
    - Implementation of procedures to restore critical electronic information systems and data within 72 hours of a loss;
    - BAs required to notify CEs upon activation of their contingency plans within 24 hours after activation.

EPSTEIN
BECKER
GREEN

Other Security Rules

Other Bills in 2023-2024 Congress

- Health Care Cybersecurity and Resiliency Act of 2024
  - Proposed legislation aimed to modernize HIPAA to better address cybersecurity threats facing health care entities. Key provisions included the development of a cybersecurity incident response plan by HHS and the creation of training programs for health care workers in collaboration with the Cybersecurity and Infrastructure Security Agency (CISA).
- Healthcare Cybersecurity Improvement Act
  - Proposed legislation would have required hospitals to establish basic cybersecurity standards as a Medicare Condition of Participation. It would have also allocated $100 million in grants to small and medium-sized hospitals to enhance cybersecurity measures and create liability protection for larger health care systems that provide smaller health care organizations access to cybersecurity resources.

CIRCIA

- Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)
  - Enacted in 2022, requires the Cybersecurity and Infrastructure Security Agency (CISA) to develop and implement regulations requiring covered entities to report covered cyber incidents and ransomware payments to CISA.
- Proposed Rule published April 2024
  - Extensive reporting obligations for entities in 16 critical infrastructure sectors including HealthCare and Public Health.
  - Covered entities required to report “substantial cyber incident” within 72 hours. “Substantial cyber incident” defined as causing any of the following:
    - Substantial loss of confidentiality, integrity, or availability
    - Serious impact on safety and resiliency of operational systems and processes
    - Disruption of ability to engage in business or industrial operations or deliver goods or services
    - Unauthorized access facilitated through or caused by a compromise of a provider or third party or a supply chain compromise
  - Covered entities also required to report a ransom payment in response to a ransomware attack within 24 hours.

CIRCIA

- Proposed Rule published April 2024 (cont'd)
  - Updates/supplemental reporting required "promptly" if "substantial new or different information becomes available" or if the covered entity makes a ransom payment after submitting a covered cyber incident report.
  - Covered entity required to preserve data relevant to the covered cyber incident or ransom payment.
- Notes for hospitals:
  - Most hospitals will be "covered entities" subject to CIRCIA.
  - Exception to reporting requirements include when entity "required by law, regulation, or contract to report substantially similar information to another Federal agency within a substantially similar timeframe" and provided that the Federal agency receiving such reports has an agreement in place to share such information with CISA. Unlikely to apply to hospitals.
  - "Substantial cyber incident" does **not** require that PHI be involved in the incident and is **not** dependent on whether the incident is a HIPAA breach.
  - 72-hour and 24-hour reporting requirements much shorter than HIPAA breach reporting.

Presented by

Lisa Pierce Reisz
614-872-2440
LPierceReisz@ebglaw.com

Allen Killworth
614-872-2415
akillworth@ebglaw.com