National Committee on Vital and Health Statistics
Advising the HHS Secretary on National Health Information Policy

NCVHS Subcommittee on Privacy, Confidentiality and Security

Recommendations to Strengthen the HIPAA Security Rule

November 29, 2023

Introduction

- NCVHS is charged with studying and identifying “privacy, confidentiality and information security measures to protect individually identifiable health information.”

- Cyberattacks increase the patient’s severity of illness due to delays in needed procedures and tests. Attacks were more likely to cause:
    - longer lengths of stay
    - increases in complications from medical procedures
    - increases in mortality rates

Charter, National Committee on Vital and Health Statistics, para. H. (Jan. 21, 2022): https://ncvhs.hhs.gov/about/charter/

Ponemon Institute on Cyberinsecurity in Healthcare: The cost and impact on patient safety and care 2023 https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-cyber-insecurity-healthcare-ponemon-report.pdf

Timeline of Past Work that Led to the Recommendations

July 14, 2021

July 20, 2022

NCVHS held hearings to better understand the cybersecurity landscape and to explore how best to protect health information and patients.

May 10, 2022

NCVHS submitted a letter: Recommendations to Strengthen Cybersecurity in Healthcare.

July 19-20, 2023

Public Meeting Presentation

Update on Privacy and Security

Director and Deputy Director

Office for Civil Rights (OCR)

September 26, 2023

The PCS Subcommittee met to address follow up questions to the Deputy Director of OCR

November 29, 2023

Recommendations to Strengthen the HIPAA Security Rule

Focus on ways to decrease cybersecurity incidents and develop a robust risk analysis

Focus on Risk Analysis

- Previously, OCR found that covered entities and business associates were not consistently compliant in implementing the Security Rule's requirements for a risk analysis and risk management program.

Focus especially on risk analysis due to:

- multiple inconsistent resources
- confusion on specific methods to employ and
- the expense for small entities and business associates

Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance For Calendar Year 2020
https://www.hhs.gov/sites/default/files/compliance-report-to-congress-2020.pdf

Proposed Recommendations 1-3

- Recommendations to Strengthen the HIPAA Security Rule
- Specifically, NCVHS recommends that HHS:

1. Require in the HIPAA security rule that all covered entities and business associates implement a security program, and that the rule specify the same minimum security controls for all covered entities and business associates.

2. Require in the HIPAA security rule that covered entities and business associates adopt a risk-based approach in their security program.

3. Include a step-by-step risk analysis procedure within the Security Rule.

Proposed Recommendations 4-6

- Recommendations to Strengthen the HIPAA Security Rule
- Specifically, NCVHS recommends that HHS:

4. Define compensating controls more specifically in the Security Rule and provide examples.

5. Reinforce the need to evaluate Artificial Intelligence (AI) systems and data within the Privacy and Security Rule as part of risk analysis for all and any new technology.

6. Standardize cyber incident reporting in the HIPAA Security Rule, and harmonize any such requirements in HIPAA rules with incident reporting provisions applicable to healthcare critical infrastructure actors and healthcare federal contractors.

Questions & Discussion