November 29, 2023

The Honorable Xavier Becerra
Secretary
Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

Re: Recommendations to Strengthen the HIPAA Security Rule

Dear Mr. Secretary:

This letter provides recommendations of the National Committee on Vital and Health Statistics on ways to enhance the cybersecurity of U.S. healthcare entities to protect the safety of patients and the reliability of lifesaving technologies in the face of a sophisticated and rapidly evolving threat landscape.

The National Committee on Vital and Health Statistics (NCVHS, the Committee) serves as your advisory body on health data, statistics, privacy, confidentiality, information security, and national health information policy. NCVHS is charged with studying and identifying "privacy, confidentiality and information security measures to protect individually identifiable health information."[1]

According to a 2022 report of the Healthcare and Public Health Sector Coordinating Council's 2023 Landscape Analysis for its Hospital Cyber Resiliency Initiative [T]he United States (U.S.) Healthcare and Public Health (HPH) sector has faced dramatic increases in cyber-attacks, causing disruption to the care continuum. The National Security Council (NSC) considers the HPH sector to be one of the top three (3) sectors prioritized for additional cybersecurity attention. This designation is consistent with other reports, such as the 2022 Verizon Data Breach Report (healthcare listed as top vulnerable sector) and the CrowdStrike 2023 Global Threat Report, which both list healthcare as the third most frequently targeted sector.[2]

In the last few years, major news outlets have even reported several patient deaths attributable to ransomware attacks.[3]

---

[1] Charter, National Committee on Vital and Health Statistics (NCVHS), para. H. (Jan. 21, 2022), https://ncvhs.hhs.gov/about/charter/.
[2] U.S. Dept. of Health and Human Services (HHS), Hospital Cyber Resiliency Initiative: Landscape Analysis (2023) https://405d.hhs.gov/Documents/405d-hospital-resiliency-analysis.pdf. *See also*, Verizon Inc., Data Breach Investigations Report (2023), https://www.verizon.com/business/resources/reports/dbir/2023/master-guide/ and CrowdStrike Inc., Global Threat Report (2023), https://www.crowdstrike.com/global-threat-report/.
[3] *See, e.g.,* Joseph Marks, "Ransomware attack might have caused another death," *Washington Post* (Oct. 1, 2021). https://www.washingtonpost.com/politics/2021/10/01/ransomware-attack-might-have-caused-another-death/

In its 2016-2017 Health Insurance Portability and Accountability Act (HIPAA) Audits Industry Report, HHS' Office for Civil Rights (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.[4] This, and the more recent news reports led the Committee to seek to understand the scope and breadth of security risks, but what we found was that not much had changed. Therefore, we began to consider how best to address those challenges in protecting the safety of patients and the healthcare system itself.

The Committee's inquiry began with a hearing on July 14, 2021, at which we heard from 11 cybersecurity experts,[5] and continued with an additional panel at the July 20, 2022, full Committee meeting with four additional experts to better understand the cybersecurity landscape and to explore how best to protect health information and patients.[6] At its full Committee meeting this past summer, the Director of OCR, Melanie Fontes Rainer, and Deputy Director for Health Information Privacy, Data, and Cybersecurity, Timothy Noonan, briefed the Committee on the second day, including cybersecurity concerns under HIPAA.[7] Members of NCVHS' Privacy, Confidentiality and Security (PCS) Subcommittee then met on September 26, 2023, to address follow up questions to the Deputy Director.

Throughout all of these meetings, the panelists and OCR officials consistently voiced their concerns about the major increase in incidents and, in particular, the widespread lack of robust risk analysis on the part of covered entities and business associates that would lead to prior planning for, and mitigation of, a range of cybersecurity threats. Based on the July 2021 hearing and subsequent discussions, NCVHS transmitted initial recommendations to you on this topic last year.[8] That letter contained four recommendations designed to strengthen the HIPAA Security Rule. Upon review of the information received by the Committee and presentations and discussions with representatives from OCR, the Committee approved further recommendations for specific actions to strengthen the Security Rule. These further recommendations focus especially on risk analysis. The Committee heard many times that risk analysis is lacking within healthcare entities due to inconsistent resources, confusion as to appropriate methods, expense for small entities and business associates, and lack of support in smaller organizations to carry out robust risk analysis. It is with this premise in mind that we make these further

---

(reporting that a ransomware attack against an Alabama hospital may have led to a baby's death in 2019 because an electronic display of fetal heart rate was unavailable to the nursing staff); William Ralston, "The untold story of a cyberattack, a hospital and a dying woman," *Wired* (Nov. 11, 2020), https://www.wired.co.uk/article/ransomware-hospital-death-germany/ (visited Dec. 17, 2023)(describing death of a patient in Germany who had to be re-routed to a new hospital after original destination experienced a cyberattack).

[4] 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.

[5] The agenda, recording, transcript, slides from the July 14, 2021, hearing, and a complete meeting summary, are available on the NCVHS website at https://ncvhs.hhs.gov/meetings/subcommittee-on-privacy-confidentiality-and-security-3/.

[6] The agenda, recording, transcript, slides from the July 20, 2022, hearing, and a complete meeting summary, are available on the NCVHS website at: https://ncvhs.hhs.gov/meetings/full-committee-meeting-11/.

[7] The agenda, recording, transcript, slides from this briefing, and a complete meeting summary, are available on the NCVHS website at: https://ncvhs.hhs.gov/meetings/full-committee-meeting-14/.

[8] NCVHS Letter to Secretary Xavier Becerra, "Recommendations to Strengthen Cybersecurity in Healthcare," (May 22, 2022) ("May 2022 Letter"): https://ncvhs.hhs.gov/wp-content/uploads/2022/05/NCVHS-Recommendations-to-Strengthen-Cybersecurity-in-HC-05-10-2022-508.pdf.

recommendations.

The stated actions strengthen the Security Rule, encouraging covered entities and their business associates to adopt strong risk management programs that include robust risk analysis. The Committee is aware that OCR has provided multiple tools and guidance on risk analysis. However, in the OCR audit findings and from the previous hearings and meetings, both covered entities and business associates failed to comply with the existing regulations.

We concluded that what constitutes an accurate and thorough enterprise-wide assessment is not clear; the guidance resources are too numerous, too voluminous, and too difficult to follow; the OCR has not made clear the significant benefits and risks, or its guidance has not been made easy enough to follow so that "friction" in adoption is less burdensome for smaller entities.

Therefore, NCVHS presents six specific recommendations that emphasize the need for risk management and risk analysis so that covered entities and their business associates mitigate critical vulnerabilities. These recommendations are based on careful consideration of the expert testimony obtained during the July 2021 and 2022 hearings, the July 19-20, 2023 presentations from OCR, discussions with representatives of OCR, published articles and reports, and the expertise of NCVHS members.

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 require the same minimum security controls for all covered entities and business associates.**
2. **Require in the HIPAA Security Rule that, in addition, covered entities and business associates adopt a risk-based approach in their security programs.**
3. **Require a step-by-step risk analysis procedure within the Security Rule that conforms with guidance from the National Institute of Standards and Technology of the Department of Commerce and the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security.**
4. **Define compensating controls more specifically in the Security Rule and provide a wider range of examples that apply to a greater variety of types of entities.**
5. **Strongly reinforce the need to account for Artificial Intelligence (AI) systems and data within the Privacy and Security Rules as part of the risk analysis for all and any new technology.**
6. **Establish a consistent floor for 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.**

Attached please find an Appendix with a detailed rationale for each of the Committee's recommendations.

Thank you for considering the recommendations in this letter. NCVHS remains available to answer questions and will continue to offer advice and support to the HHS efforts to strengthen health information security and protect the safety and health of all Americans.

Sincerely,

/s/

Jacki Monson, J.D., Chair
National Committee on Vital and Health Statistics

Enclosure

Appendix: Rationale for NCVHS Recommendations to Strengthen the HIPAA Security Rule

APPENDIX

Rationale for NCVHS Recommendations to Strengthen the HIPAA Security Rule

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 require the same minimum security controls for all covered entities and business associates.**

   The Committee recommends that HHS eliminate the ability of a covered entity or business associate to avoid adopting any solution under the HIPAA Security Rule's "addressable" (recommended but voluntary) implementation specifications. Rather, covered entities and business associates should be required either to be in full compliance or to adopt a reasonable documented alternative. The Security Rule should set minimum security controls for covered entities and business associates such as the new requirements described below:

   - designation of a qualified information security official
   - elimination of default passwords
   - adoption of multi-factor authentication
   - institution of offline backups
   - installation of critical patches within a reasonable time and
   - transparency of impact and vulnerability disclosures

   More detail regarding each of these security controls is provided in the Committee's Cybersecurity letter of May 2022.[9] The Office for Civil Rights (OCR) previously mapped the HIPAA Security Rule requirements to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) subcategories and corresponding security controls derived from NIST Special Publication 800-53 Revision 5.[10] We recommend this mapping be updated within a specific time period once version 2.0 of the NIST CSF is finalized (scheduled to be published in early 2024), from which minimum requirements may be derived.[11] In case applicable minimum control requirements are not specified, they should be considered as checklist requirements for HIPAA security risk assessments.

---

[9] May 2022 Letter, pp. 5-9.

[10] Nat'l Inst. Of Standards and Tech., Dept of Comm., Special Publication SP 800-53, Rev. 5, "Security and Privacy Controls for Information Systems and Organizations (Dec. 10, 2020, with updates to the "Mappings and crosswalks" text and links on Dec. 19, 20230, https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final (visited Dec. 19, 2023).

[11] See the following additional sources that should be considered for minimum requirements: NIST SP 800-207 "Zero Trust Architecture" (Aug. 2020) https://csrc.nist.gov/pubs/sp/800/207/final; NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management (Jan. 16, 2020), https://www.nist.gov/privacy-framework; NIST SP 800-151 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (May 2022), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf; NIST Artificial Intelligence Risk Management Framework (Jan. 23, 2023), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf; American Institute of Certified Public Accountants (AICPA) Service Organizations (SOC 2): Trust Services Criteria, and; Health Information Trust Alliance (HITRUST) Common Security Framework (CSF).

Minimum encryption requirements for data security and use of crypto agility

In 2023, a vendor (MOVEit) failed to patch and encrypt data at rest that lead to PHI (name and date of birth, health insurance information, provider name, treatment cost information and treatment information or diagnosis) being impacted.[12] It was reported that several federal government agencies were also hit by cyber-attackers who targeted MOVEit, along with "several hundred" companies and organizations.[13] Implementing the White House National Security Memorandum[14] of May 4, 2022, including applicable NIST guidance[15] on vulnerable cryptographic systems is necessary to strengthen the Technical Safeguards within the Security Rule. While security of data-in-transit is covered in the current Security Rule, ensuring that data-at-rest is also secure is equally important.

Both data-at-rest and data-in-transit must be ready for emerging quantum computing (QC)-related threats. The mechanics of quantum computing can solve complex problems, such as the algorithm behind encryption keys that protect health data, that are too difficult for the classical computer to decipher. The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and NIST published a factsheet about the impacts of quantum capabilities. The agencies urge all organizations to begin early planning for migration to post-quantum cryptographic (PQC) standards by developing their own quantum-readiness roadmap.[16] As a first step, organizations must implement a robust risk analysis program that begins with an inventory of the cryptographic technology used in all systems, both for data-in-transit and data-at-rest. All systems using cryptographic technology should have a known risk classification so that higher-risk systems may be upgraded more urgently when needed. All encryption solutions must meet the minimum encryption and hashing algorithm standards that do not currently have any vulnerabilities. To be ready for QC threats, technology solutions must have a planned upgrade path to the NIST QC-resistant crypto-suite based on their risk rating.

Recommended security practices for securing cloud computing services

The Security Rule was promulgated before the adoption and implementation of cloud computing services. Cloud computing technology can provide convenient, on-demand network access to a shared pool of computing resources (e.g., networks, servers, storage, applications, and services).[17] Cloud technology may be managed locally on covered entity or business associate premises or remotely by a Cloud Service Provider (CSP). However, if an entity uses a CSP, there are additional considerations to ensure security of the covered entity's ePHI. Most healthcare organizations now

[12] Sutter Health vendor data breach exposes personal information of more than 845,000 patients (msn.com).
[13] US government agencies hit in global cyberattack (kcra.com) FIND A MORE RELIABLE SOURCE – and see Rec 4.
[14] National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems | The White House.
[15] Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography (nist.gov).
[16] CISA, NSA and NIST Publish New Resource for Migrating to Post-Quantum Cryptography https://www.cisa.gov/news-events/news/cisa-nsa-and-nist-publish-new-resource-migrating-post-quantum-cryptography.
[17] NIST SP 800-145, The NIST Definition of Cloud Computing https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

use cloud computing services such as infrastructure-as-a-service (IaaS), platforms-as-a-service (PaaS), or software-as-a-service (SaaS). Appropriate security practices should be implemented in order to protect ePHI, to avoid loss of data in the cloud, or to avoid other misuse of cloud assets. A major step in risk analysis includes identifying vulnerabilities, and this is necessary for the management of cloud assets as well. All technical and administrative controls must apply to mitigate the following risk factors:

- Data breaches — unauthorized access to sensitive data stored in the cloud.
- Misconfiguration — improper settings of cloud resources that expose them to attacks. There are unique configuration challenges with CSPs since one does not have the hardware and software under the covered entity's control. The default parameters often are assigned by the third party and may require extra steps taken by expert staff to secure the covered entity's data.
- Insecure Application Programming Interfaces (APIs) — vulnerable interfaces that allow attackers to manipulate cloud services.
- Distributed Denial of Service (DDoS) attacks — overwhelming cloud servers with network traffic to disrupt their availability.
- Hijacking of accounts — stealing credentials or tokens to gain control over cloud accounts.
- Inadequate training: lack of awareness or skills among cloud users or providers to follow security best practices.
- Inadequate knowledge of service agreements about data use for vendor improvement of systems or inadequate security requirements by subcontractors or third parties that are not explicitly covered entities.

The Federal Risk and Authorization Management Program (FedRAMP) authorizes CSPs for use by federal agencies and in agency contracts by providing a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP is mandatory for all executive agency cloud deployments. OCR should consider the benefits of FedRAMP assessment requirements as a standard in the HIPAA Security rule. One option for meeting the standard would be to select as one's vendor a CSP holding an authorization in the FedRAMP Marketplace for the appropriate level of risk to be managed. Selecting a vendor from the FedRAMP marketplace is a more efficient and less expensive way of meeting the assessment requirements for the use of cloud services. As part of a business associate agreement (BAA), a covered entity could negotiate with their business associate to ensure using only FedRAMP compliant CSPs.

Network Security: Network Segmentation based on user characteristics

Healthcare organizations should adopt defense-in-depth (DID) to protect ePHI across the network, including network segmentation based on user characteristics (e.g. employee vs contractor). DID, as defined by NIST, is the application of multiple countermeasures in a layered or stepwise manner to achieve security objectives.[18] Layered security controls — multiple layers to protect your most important assets — are critically important to protect network security. This must include segregation between, for example, a corporate network, internet facing applications, third party vendors, and business associates.

[18] NIST Glossary Defense in Depth https://csrc.nist.gov/glossary/term/defense_in_depth.

Application Programming Interface (API) Security

Application Programming Interface Security is currently an addressable Technical Safeguard within the Security Rule. APIs, including Health Level 7 (HL7) Fast Healthcare Interoperability Resources (FHIR)-based APIs and others required of health plans and health care providers by federal and state regulations, raise security problems. Ransomware is one of the most serious concerns about API security because attackers can exploit insecure APIs to obtain access to and then encrypt healthcare data, thus facilitating effective ransomware assaults. Unauthorized access due to API exploits can pose additional hazards to individuals and healthcare systems. At times, APIs may not limit access to ePHI to the minimum necessary nor to data elements specified in contracts or BAAs. Although it may be expensive for smaller organizations, auditing to ensure that what was authorized or intended to be disclosed is what was actually disclosed is a vital security practice. In order to implement this requirement successfully, another government entity, such as the Centers for Medicare and Medicaid Services (CMS), may need to offer an incentive. Cloud services frequently make use of APIs. APIs enable access to health data including ePHI, which must be protected by authentication, authorization, and encryption controls.

2. **Require in the HIPAA Security Rule that, in addition, covered entities and business associates adopt a risk-based approach in their security program.**

   NCVHS recommends that minimum security requirements, including applicable security program components such as data access controls, encryption, and breach response plans, apply to all covered entities and business associates holding PHI. We further recommend that all business associates, subcontractors, and other vendors have a documented security management program that includes risk analysis. Historically, there have been many addressable items in the Security Rule that permit mere attestation of compliance, but that has proven insufficient to ensure that entities large or small have effective data security programs.

   To mitigate potential burdens, covered entities and business associates with fewer records and a lesser scope of PHI should use a risk-based approach to implement security controls and compensating controls, commensurate with the risk of damage or harms. OCR's Guidance should specify acceptable options for these security controls.

3. **Require a step-by-step risk analysis procedure within the Security Rule that conforms with guidance from the National Institute of Standards and Technology of the Department of Commerce and the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security.**

   Information from all of the guidance documents from NIST, CMS, and OCR as well as OCR's Cybersecurity newsletters[19] should be compiled into a simple step-by-step risk analysis procedure that both small and large covered entities and business associates can use to perform risk analysis, including risks posed by sub-contractors and other vendors. This will help to reduce ambiguity and to improve effectiveness of compliance for covered entities and business associates.

[19] *See, e.g.*, the most recent OCR Cybersecurity Newsletter available at the time of the Committee's recommendations, OCR, HHS, "How Sanction Policies Can Support HIPAA Compliance," (October 2023), https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-october-2023/index.html (visited Dec. 29, 2023).

The Committee proposes examples of the basic steps that should be included in the risk analysis procedure. The goal is to make sure that minimum risk analysis requirements are understandable, are feasible in their implementation based on risk, and facilitate better compliance. It may be helpful for OCR to circulate a draft to a diverse sample of entities for comment. Once finalized, OCR should amend the Security Rule provisions that are found to be the most helpful for covered entities and business associates, in plain language so that they can easily comply. Listed below are the steps that the Committee recommends be included in the risk analysis procedure:

1. Characterize the System — identify where all PHI is stored and collect data on applications and systems used by the organization so that a systems inventory is created.
2. Identify and Document Potential Threats and Vulnerabilities — consider acts of nature, environmental threats, technology associated threats, acts of individuals etc.
3. Assess Current Security Measures — identify the controls that are already in place. These may differ between smaller and larger entities and between an organization with few records as compared to one with many records.
4. Assess the applicability of existing health care cybersecurity standards.[20]
5. Determine the Likelihood of Threat Occurrence — assess and identify what controls are missing and the means by which applications and systems can be exploited.
6. Determine the Potential Impact of Threat Occurrence — assess the probability that each threat could occur and the magnitude of the potential impact in all areas.
7. Determine the Level of Risk — calculate a risk score that is based on the likelihood that the system will experience the threat with the current controls in place, and estimate the impact to the entity, e.g., likelihood x impact = risk score.
8. Document Results — record assigned risk levels and produce a list of corrective actions to mitigate each risk level.
9. Finalize Documentation — the risk analysis documentation is a direct input to the risk management process.
10. Specify Periodic Review and Updates to the Risk Assessment — conduct continuous risk analysis to identify when updates are needed. Risk analysis should be performed as new technologies and business operations are planned, so that potential risks are mitigated before that new technology or business operation is put into place. Apply "security by design"[21] principles to system development and maintenance activities frequently to assist ongoing updates.[22]

---

[20] Some examples of the types of standards we have in mind include: NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations; NIST SP 800-171 Rev. 2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final (visited Dec. 29, 2023); Int'l Org. for Standardization (ISO)/Int'l Elec. Comm. (IEC) 27001, Information Security, Cybersecurity and Privacy Protection, Information Security Management Systems Requirements; ISO/IEC 27002, *Information Security, Cybersecurity and Privacy Protection, Information Security Controls*, https://www.iso.org/standard/27001 (visited Dec. 29, 2023); HHS Ofc. of Info. Sec. 405(d) *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients* (HICP 2023 Edition) https://405d.hhs.gov/Documents/HICP-Main-508.pdf (visited Dec. 29, 2023); Payment Card Ind. Data Sec. Standards (PCI-DSS) PCI DSS v4.0 Quick Reference Guide https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/PCI_DSS-QRG-v4_0.pdf; HL7 FHIR standards,https://build.fhir.org/ig/HL7/fhir-pacio-rt/security_and_privacy.html.

[21] https://www.cisa.gov/securebydesign.

[22] *See* OCR, HHS, *Guidance on Risk Analysis* (July 22, 2019),

11. Test to Produce Evidence of Compliance — test at multiple points in the life cycle of a system, including prior to production, routinely during production, at every significant change throughout the life of the system, and at system retirement.
12. Produce an Assessment of the Business Continuity and Resiliency plan — plan for both short-term and extended system outages. This enables the healthcare organization to be flexible and to respond quickly to both known and unknown risks.

4. Define compensating controls more specifically in the Security Rule and provide a wider range of examples that apply to a greater variety of types of entities.

Hackers can get into a system and nest there for several months without the awareness of the covered entity and business associate. This can lead to exfiltrating data on a daily basis. The system can still be putting out alerts, but since there is no regular review to respond and no audit controls, it becomes extremely difficult to know where the impact is. This happened to Anthem on March 13, 2015. Anthem filed a breach report on January 29, 2015, that they discovered cyber-attackers had gained access to their IT system via an undetected continuous and targeted cyberattack. Anthem found that the cyber-attackers had infiltrated their system through spear phishing emails. OCR's investigation revealed that between December 2, 2014, and January 27, 2015, the cyber-attackers stole the ePHI of almost 79 million individuals, including names, social security numbers, medical identification numbers, addresses, dates of birth, email addresses, and employment information. In addition to disclosure of ePHI, OCR found that Anthem did not conduct an enterprise-wide risk analysis, had insufficient procedures to regularly review information system activity, failed to identify and respond to suspected or known security incidents, and failed to implement adequate minimum access controls to prevent the cyber-attackers from accessing sensitive ePHI, beginning as early as February 18, 2014. In addition to the $16 million settlement, Anthem performed a robust corrective action plan to comply with the HIPAA Rules.[23]

The entire state of Maine was impacted on May 28-31, 2023, due to a software vulnerability in MOVEit that allowed a group of cybercriminals to access and download files belonging to Maine state agencies. This incident was specific to the MOVEit server and demonstrates how cybercriminals can get into a system and stay there without the awareness of the covered entity and business associate and how regular reviews and audit controls are needed to respond effectively.[24]

Compensating controls are those controls that can be put in place by covered entities and business associates as an alternative control when the original control is too burdensome or costly. Compensating controls should still have the same or greater effect in safeguarding ePHI as a recommended control and can improve clarity, reduce burden, and avoid prohibitive expense in

---

https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html (visited Dec. 29, 2023); Walsh, Tom. "Security Risk Analysis and Management: An Overview," AHIMA Practice Brief(Nov. 2013); OCR, HHS, "HIPAA Security Rule Security Incident Procedures," (Oct. 2022). https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-october-2022/index.html (visited Dec. 29, 2023).

[23] US Dept HHS Guidance Portal--Anthem Pays OCR $16 Million in Record HIPAA Settlement Following Largest U.S. Health Data Breach in History https://www.hhs.gov/guidance/document/anthem-pays-ocr-16-million-record-hipaa-settlement-following-largest-us-health-data-breach.

[24] MOVEit Global Security Incident https://www.maine.gov/moveit-global-data-security-incident/#:~:text=The%20software%20vulnerability%20was%20exploited,%2C%20and%20May%2029%2C%202023.

security control implementation. Many times the compensating controls are used with legacy systems. OCR provides examples of how to strengthen existing controls or use compensating controls outlined below.[25] It is important that those controls combat potential risk and vulnerabilities identified with a legacy system or any system:

- Enhancing system activity reviews and audit logging to detect unauthorized activity, with special attention paid to security configurations, authentication events, and access to ePHI.
- Restricting access to the legacy system to a reduced number of users.
- Strengthening authentication requirements and access controls.
- Restricting the legacy system from performing functions or operations that are not strictly necessary (e.g., by removing or disabling unnecessary software and services).
- Ensuring that the legacy system is backed-up – especially if strengthened or compensating controls impact prior backup solutions.
- Developing contingency plans that contemplate a higher likelihood of failure, especially if the legacy system is providing a critical service.
- Implementing aggressive firewall rules.
- Implementing supported anti-malware and next generation anti-virus solutions.

While these examples are helpful for some organizations to use, it is recommended that HHS consider providing additional examples that can serve a wide variety of covered entities and business associates since the burden and cost of doing some of these activities may not be possible and these entities would welcome specific examples of what worked for other similar organizations. Both large and small organizations should have additional examples of compensating controls that might reduce the cost burden of System Activity Reviews (SARs) when conditions may render compensating controls appropriate. SARs include activity event logs and alerts, and security activity logs for systems and devices, which are monitored, collected, reviewed, analyzed, stored, and reported as audit records. It should be included in the Security Rule that activity logs, time stamps, settings, and reports should be protected from unauthorized access, modification, or deletion with access restrictions. Also, all personnel should be trained to do the above and to identify and report potential security and compliance incidents, or initiate investigations.

5. Strongly reinforce the need to account for Artificial Intelligence (AI) systems and data within the Privacy and Security Rules as part of the risk analysis for all and any new technology.

AI's introduction into the healthcare system has been in the context of improving performance, capacity, and efficacy of healthcare services particularly in the area of clinical decision support systems. Machine learning approaches are being employed to develop predictive models that include disease diagnosis to a patient's treatment. AI tools including large language models and chatbots are innovative software tools that can assist with many clinical management operations, predict patient risk, enhance workflow, assist in healthcare decision making, identify billing codes, and respond to messages in a patient portal.[26] However, there are also many risks associated with these AI tools such as the risk to privacy and security of ePHI as well as a "crucial need for Privacy-Preserving Machine Learning (PPML) in healthcare to enable the implementation of trust-worthy

[25] Fall 2021 OCR Cybersecurity Newsletter OCR Cybersecurity Newsletter: Securing Your Legacy [System Security] https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-fall-2021/index.html.
[26] Privacy-preserving artificial intelligence in healthcare: Techniques and applications 2023

systems in the future."[27]

For example, when using, ChatGPT, one of the most well-known generative AI applications based on a large language model, ePHI will flow to an outside organization called OpenAI, and in most cases a BAA may not be signed so this could lead to unauthorized disclosure under HIPAA.[28] Also, a covered entity should conduct a system evaluation on all but especially any new technology to an IT system and that begins with risk analysis. However, many organizations may not think to conduct this type of evaluation with an AI tool or request information about security issues when purchasing such tools. AI solutions are dependent on aggregation and organization of training data. The biggest threats to AI are found in input data and data poisoning (for example, fictitious/poor quality data fed into the system can change a learning model over time). AI tools can create mass scale cyber-attacks that are highly effective and major threats to ePHI.[29] In the near future, AI tools will publish exploits to weaponize threats against newly published software almost instantaneously so covered entities will need AI to defend timely (e.g. hourly).[30]

The use of model data poses unique risks that can affect the outcome of the use of AI. The data that forms the model must be protected as carefully as other protected data. An intruder or adversarial actor could introduce incorrect data that would bias a model, produce incorrect results, and eventually cause misdiagnoses or inappropriate recommendations for treatment. For example, UnitedHealthcare's use of the nH Predict AI model has a 90 percent error rate and overrides physicians' recommendations for medically necessary post-acute care for the elderly.[31]

Therefore, the Committee recommends OCR publish clarifications detailing how HIPAA rules apply to AI systems. For example, AI training data, prediction models, and algorithm data should be required to be protected by administrative safeguards including Data Protection, Information Access Management, and Security Management Process controls. In the current environment of rapidly changing pervasive AI, regulators should make compliance mandatory for high-risk uses of AI where attacks would have severe societal and financial consequences. Consider use of synthetic data. Compliance should be modified for lower risk in line with the potential lower risk consequence of the prediction of disease diagnosis or treatment plans.

Part of the Security Management Process controls can begin with risk analysis by assessing what data the AI tool has access to, where the data is disclosed and where the output goes. It is then important to assess who has access, what controls are in place, whether there is a BAA and what limitations are included in the BAA, what is the AI trained on and what is the output. Since AI tools change over time, risk analysis should be conducted each time the AI is upgraded, or if the organization who owns it changes, or when changing data patterns may indicate that algorithms should be reviewed. Therefore, it is important to conduct risk analysis on AI throughout the life-cycle of the system.

---

[27] Privacy-preserving machine learning for healthcare: Open challenges and future perspectives 2023 https://openreview.net/pdf?id=4hsS1gZlPzW.

[28] Kanter GP, Packel EA. Health Care Privacy Risks of AI Chatbots. JAMA. 2023;330(4):311–312. doi:10.1001/jama.2023.9618.

[29] 3 ways AI will change the nature of cyber-attacks | World Economic Forum (weforum.org).

[30] https://www.technologyreview.com/2021/04/08/1021696/preparing-for-ai-enabled-cyberattacks/.

[31] UnitedHealthcare Faces Legal Battle Over Faulty AI Model Denying Seniors' Medical Claims (msn.com).

6. **Establish a consistent floor for 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.**

The Healthcare and Public Health (HPH) sector is one of the 16 critical infrastructure sectors comprised of sector owners and operators. Healthcare entities are directed by Presidential Policy Directive 21[32] and the National Defense Authorization Act of 2021[33] to protect essential healthcare and public health assets and services from existential threats. HIPAA covered entities are important actors in this critical infrastructure sector. As federal agencies promulgate cyber incident reporting rules applicable to subsets of this sector it will be helpful for HIPAA regulations to provide a common baseline of requirements for all covered entities and business associates.

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA),[34] among other things, 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. These reports will allow CISA to rapidly deploy resources and render assistance to victims suffering attacks, analyze incoming reporting across sectors to spot trends, and quickly share that information with network defenders to warn other potential victims. At present, in advance of these regulations, CISA provides guidance[35] specifying ten data elements to share in cyber incident reporting, along with reporting forms[36] and definitions[37]:

1. Incident date and time
2. Incident location
3. Type of observed activity
4. Detailed narrative of the event
5. Number of people or systems affected
6. Company/Organization name
7. Point of Contact details
8. Severity of event
9. Critical Infrastructure Sector if known
10. Anyone else you informed

Separately, Federal Acquisition Regulation (FAR) proposed revisions would develop standardized contract language for cybersecurity requirements, along with additional information sharing and cyber threat reporting measures. The proposed revision to FAR essentially describes two new rules relevant to government healthcare contracts, e.g. for Medicare or Tricare health plans and providers:

1. Cyber Threat and Incident Reporting and Information Sharing, which imposes cyber incident reporting requirements on federal contractors, and;

---

[32] https://www.cisa.gov/resources-tools/resources/presidential-policy-directive-ppd-21-critical-infrastructure-security-and

[33] https://www.congress.gov/116/bills/hr6395/BILLS-116hr6395enr.pdf.

[34] https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia.

[35] Sharing Cyber Event Information With CISA: Observe, Act, Report.

[36] Report to CISA | CISA Incident Reporting Form.

[37] Computer Security Incident Handling Guide (nist.gov).

2. Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems, which further clarify cybersecurity contractual requirements for federal contractors managing government unclassified information.

These two new proposed rules, if adopted as drafted, would represent material changes to the cyber compliance and reporting landscape. Some of the proposed rules significantly impact most covered entities with additional obligations to comply with the enhanced cybersecurity requirements for incident reporting, information sharing, and granting federal government (or its designees) full access to information and information systems in the event of a security incident. For example:

- Under the proposed guidelines, contractors would be required to develop and maintain software bills of materials (SBOMs) for all software used as part of a federal contract.
- The FAR revisions would require contractors to implement and leverage comprehensive cybersecurity frameworks that help protect information systems. Contractors would also have to prove they meet specific requirements for individual procurements and to work with and maintain high-value systems.

Healthcare entities must consider the changes that may be required for their policies and processes when the above rules are finalized to prepare for updating their cybersecurity controls and compliance processes. Provisions of the HIPAA Security Rule should be the central source of cyber security requirements for covered entities and business associates.