ConnectedHealthInitiative

March 7, 2025

The Honorable Robert Kennedy, Jr.
Secretary of Health and Human Services
200 Independence Avenue Southwest
Washington, District of Columbia 20201

Anthony Archeval
Acting Director for Office for Civil Rights
200 Independence Avenue Southwest
Washington, District of Columbia 20201

RE: Comments of the Connected Health Initiative, HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information [HHS-OCR-2024-30983; 90 FR 898]

Dear Secretary Kennedy and Acting Director Archeval:

The Connected Health Initiative (CHI) appreciates the opportunity to respond to the Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) on its proposal to modify the Security Standards for the Protection of Electronic Protected Health Information ("Security Rule") under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act), revising existing standards to "better protect the confidentiality, integrity, and availability of electronic protected health information (ePHI)" to address changes in the environment in which health care is provided; significant increases in breaches and cyberattacks; common deficiencies the Office for Civil Rights has observed in investigations into Security Rule compliance by covered entities and their business associates (collectively, "regulated entities"); other cybersecurity guidelines, best practices, methodologies, procedures, and processes; and court decisions that affect enforcement of the Security Rule.[1]

I. Introduction & Statement of Interest

CHI is the leading effort by stakeholders across the connected health ecosystem to enable the responsible deployment and use of digital health tools throughout the continuum of care, supporting an environment in which patients and consumers can see improvements in their health. Across a range of touchpoints in the healthcare ecosystem, we seek essential policy changes that will enable all Americans to realize the benefits of an information and communications technology-enabled American healthcare system. For more information, see www.connectedhi.com.

[1] 90 FR 898.

II. The Connected Health Initiative's Commitment to Protecting Sensitive Health Data and the Need for Clarity Under HIPAA

No data is more personal to Americans than their own health data, particularly for sensitive areas such as reproductive health. CHI members acknowledge and respect the significant threats to Americans' most sensitive data and put extensive resources into ensuring the security and privacy of health data to earn the trust of consumers, hospital systems, and providers.

The HIPAA privacy and security rules provide a set of minimum standards for protecting all electronic PHI that a covered entity and business associate create, receive, maintain, or transmit.[2] The concerns addressed by these laws are taken seriously by CHI members, who in turn work to meet the letter and spirit of the law. However, HIPAA privacy and security rules and guidance applicable to basic modern technology modalities, such as mobile apps, have fallen woefully out of touch with today's technology, and the persistent lack of clarity around HIPAA applicability in a mobile environment prevents many patients from benefiting from these services. As a result, many providers and patients find themselves discouraged from leveraging basic technologies. While OCR has developed a limited audit program in sub-regulatory guidance for assessing covered entities' controls and processes,[3] and HHS has issued guidance with specific scenarios which may be helpful in a narrow range of circumstances,[4] regulatory relief, or, at minimum, more guidance, is needed to address the use of new innovative modalities and software app-powered products and services that facilitate the flow of PHI.

CHI believes that as OCR continues to work to improve the HIPAA rules to meet the needs of our changing industry and standards of care, it is imperative that OCR continues to work to ensure that the HIPAA rules do not unduly restrict the ability of covered entities and their business associates to use the most efficient and secure technologies in their operations. CHI has detailed many ways that OCR can improve HIPAA rules to advance connected care while protecting patient privacy in previous public comments,[5] which we urge OCR to consider acting consistent with in this matter and its general efforts to modernize HIPAA regulations.

[2] 45 CFR Part 160; 45 CFR Part 164 Subparts A and C.

[3] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html.

[4] http://hipaaqsportal.hhs.gov/a/pages/helpful-links.

[5] CHI comments to OCR detailing the range of ways that HIPAA regulations should be updated to protect patients while enabling the use of new technologies can be found at https://www.regulations.gov/comment/HHS-OCR-2018-0028-1188.

III. Connected Health Initiative Input on Proposed HIPAA Security Rule Changes

The Connected Health Initiative recognizes the importance of modernizing cybersecurity standards in the healthcare sector. However, the current proposals are overly complex and fail to account for the diverse landscape of HIPAA covered entities (CEs). Not all CEs operate at the same scale, pose the same level of risk, or have the resources to comply with uniform, one-size-fits-all regulations.

Smaller healthcare organizations and digital health innovators often operate with limited resources and already face significant compliance challenges. For example, smaller entities continue to feel the impacts of the Change Healthcare Corporation breach.[6] Any updates to the HIPAA Security Rule must appropriately allocate risk and regulatory burden, taking into account the vast differences in operational capacity and technological sophistication among covered entities.

The Biden Administration's Proposed Rule, as currently drafted, requires substantial revision. If finalized in its current form, it would impose excessive compliance burdens on under-resourced entities without delivering a corresponding benefit to the security of electronic PHI (ePHI) for patients, providers, and CEs alike. A more balanced approach is necessary—one that enhances security while fostering innovation and ensuring that all stakeholders, regardless of size, can continue delivering high-quality, connected healthcare solutions.

Noting our general support for OCR's goals, we offer the following recommendations on its proposals:

Ensuring Sufficient Time for CE Compliance

OCR currently proposes that CEs would have 180 days after the effective date to come into compliance with the final rule. This would provide CEs a mere eight months to undertake the necessary investments and operational changes to comply. We are concerned that this timeline is too short given the complexity of the proposed changes and request that OCR extend the compliance date to 365 days. This will allow CEs, including those that are under-resourced, greater runway to take the necessary steps to ensure compliance.

[6]

Needed Definitional and Compliance Metric Clarifications

CHI urges OCR to provide greater clarity and practical guidance regarding the newly introduced definitions and compliance expectations in the Proposed Rule. CHI recommends the following refinements and support measures:

Effective Technical Policies: To harmonize the application technical policies across their organizations. OCR should:

- Provide scalable, practical guidance tailored for small and resource-limited healthcare providers.
- Develop low-cost or no-cost implementation tools, such as templates, checklists, and automated policy enforcement mechanisms, to help smaller entities establish effective safeguards.
- Encourage collaboration with health IT vendors to ensure they provide built-in policy enforcement features.

Defining "Reasonable Safeguards" with Clear Metrics: The Proposed Rule introduces expectations for "reasonable safeguards" but lacks clear, objective metrics for assessing compliance. Without standardized criteria, enforcement could be inconsistent and unpredictable. OCR should:

- Define specific benchmarks for evaluating whether safeguards are functioning as intended, reducing ambiguity for regulated entities.
- Provide real-world case studies and compliance examples to illustrate best practices.
- Establish a standardized audit framework to ensure fair and consistent enforcement.
- Avoid making all specifications required and retain the current treatment of some as "addressable." Where appropriate, specify that CEs may determine whether a specification is "reasonable and appropriate" for its environment and, if not, allow CEs to provide a justification for using a different method to achieve a desired outcome. Adoption of "reasonable and appropriate" qualifiers throughout the proposed rule will enable CEs to adopt a more flexible and risk-based approach consistent with existing operations.

Risk Analysis Framework Adaptation: OCR's eight-step risk analysis framework is a valuable tool for identifying and mitigating threats but is overly complex and not appropriate for all technologies and assets subject to the Security Rule. These practices require streamlined, practical solutions to implement cybersecurity best practices effectively. OCR should:

- Develop simplified risk analysis templates and assessment tools that allow small entities to comply without requiring extensive cybersecurity expertise.
- Provide tiered compliance options that recognize the resource limitations of smaller practices while maintaining strong security standards.

- Work with industry stakeholders and professional associations to create user-friendly risk management frameworks that align with real-world workflows.

Clarifying Technical Controls and Definitions: Generally, OCR should establish definitions that promote the adoption of innovative technologies and advancements in security standards while avoiding the risk of obsolescence. Where appropriate, definitions should allow regulated entities to implement reasonable and appropriate measures to ensure the security of health data. Notable needed updates in OCR's proposed definitions include:

- Defining "Security Incident": We propose removing unsuccessful attempts from the definition of a "Security Incident." In fact, these failed attempts demonstrate that security controls are functioning effectively. Documenting every failed attempt as a security incident is impractical due to the high volume of attempts many Business Associates (Bas) experience.
- Defining "Relevant Electronic Information System": The proposed definition is overly broad, encompassing any "electronic information system that […] otherwise affects the security of PHI." This could lead to interpretations that impose stringent requirements on systems with only a minimal or theoretical connection to PHI security. Additionally, regulated entities, particularly those utilizing cloud computing or shared services, may lack direct responsibility or control over all electronic information systems that might impact PHI security.
- Defining "Workstation": The definition of "workstation" should be refined to include "electronic storage material" connected to and used with an electronic computing device. More clarity is needed to prevent unnecessarily broadening the scope of devices that fall under the Security Rule's workstation requirements. Ambiguities regarding the "immediate environment" could inadvertently include systems not directly related to the security of patient information.

Considering the definitions of "relevant electronic information system" and "workstation," CHI has concerns about the proposed penetration testing requirements. If finalized, these definitions could encompass a much wider range of systems and assets than intended, making them subject to the parallel penetration testing requirements. We recommend that OCR incorporate a reasonable and appropriate qualifier for penetration testing based on assessed risk.

Network Segmentation Support for Small Practices: Network segmentation is a critical cybersecurity measure to limit unauthorized access to ePHI, but small practices often lack the technical expertise to implement it effectively. Many rely on third-party vendors and IT providers for network security. To ensure feasible compliance, OCR should:

- Provide clear implementation guides and best practices tailored for small healthcare organizations with limited IT resources.
- Encourage health IT vendors to offer built-in segmentation capabilities.

- Offer technical assistance programs and financial incentives to help small practices upgrade their network infrastructure for improved security.

Revisions Needed to Align OCR's Proposal with Risk-based Standards and Scale Requirements for ePHI

OCR should ensure that the proposed rule is technology-neutral and aligns more closely with current security standards. Cybersecurity standards typically prioritize achieving specific security outcomes rather than dictating the methods that CEs must use to achieve those outcomes. Prescriptive technical requirements can increase the burden on regulated entities and create discrepancies between the Security Rule and widely accepted industry standards. Focusing on specific methods for achieving security outcomes may inadvertently overlook or exclude new technologies that can deliver the same results. OCR should clarify that regulated entities need to evaluate whether a specification is reasonable and appropriate for their environment; if it is not, they should provide a justification for using an alternative method to achieve the desired outcome.

CHI recognizes the urgent need to strengthen cybersecurity across the healthcare sector. However, the Proposed Rule imposes overly burdensome requirements on all CEs and BAs, regardless of size, operational capacity, or risk profile. Compliance with these new standards would require significant resource investment, disproportionately impacting smaller healthcare providers and digital health innovators. While we agree that healthcare cybersecurity must be improved, a one-size-fits-all approach is not the solution. A nuanced approach that accounts for the unique needs of all HIPAA-covered entities will better position stakeholders to mitigate the most serious risks that could precede a significantly disruptive cybersecurity event.

Despite this, the Proposed Rule mandates that all regulated entities adhere to the same cybersecurity requirements, without flexibility based on organizational size, resources, or risk assessment. This means that small, resource-constrained entities must meet the same cybersecurity standards as the largest health plans and clearinghouses. Additional regulatory burdens would divert limited time and funds away from patient care and efforts to innovate care delivery models, further straining an already overstretched workforce. OCR must revise the Security Rule to establish a risk-based framework that considers the attack surface of a given entity and assesses the potential impact of a breach on industry-wide operations. Such an approach would be consistent with:

- The recently proposed CIRCIA Reporting Requirements, which appropriately distinguish between large and small entities when determining cybersecurity reporting obligations. CIRCIA focuses regulatory efforts on larger organizations that pose a significant risk to critical infrastructure, ensuring that cybersecurity requirements are proportional to the potential threat of industry disruption. A similar risk-based approach should be applied to the HIPAA Security Rule.

- OCR's Section 1557 Rules, which modifies Section 1557 of the Affordable Care Act, provides a strong precedent for a differentiated regulatory approach. Under 45 C.F.R. §92.210(b), Covered Entities (CEs) must make "reasonable efforts" to identify the use of patient care decision-support tools in their health programs or activities. OCR has clarified that it will assess these efforts based on an entity's size and resources—acknowledging that a large hospital with dedicated IT staff has far greater capacity than a small provider without such resources.

Preserve Flexibility for Regulated Entities Based on Risk and Organizational Needs

The Connected Health Initiative urges OCR to retain the built-in flexibilities of the current HIPAA Security Rule, which allows regulated entities to implement cybersecurity safeguards in a way that aligns with their specific risks, resources, and operational realities. The existing HIPAA Security Rule, finalized in 2003, includes both "required" and "addressable" implementation specifications. While required specifications must be followed by all entities, addressable specifications provide organizations with flexibility, allowing them to determine whether a specific measure is reasonable and appropriate based on their risk assessment. If a specification is not deemed appropriate, entities must document their reasoning and implement an equivalent alternative measure when feasible.

The Proposed Rule removes these addressable implementation specifications, instead mandating compliance with all new requirements without consideration of an entity's specific situation. This shift ignores the realities faced by small and under-resourced entities. Without the flexibility to tailor security measures, many of these small entities may be forced to contract with expensive outside consultants just to meet the new requirements. Noting its commitment to enhancing cybersecurity as a patient safety issue and protecting electronic protected health information (ePHI), CHI urges OCR to provide needed flexibility to implement safeguards that make sense for their size, infrastructure, and risk profile.

New Rules Would Impose Excessive Administrative Burdens Without Clear Benefit

One of the most problematic new mandates in the Proposed Rule is the requirement for a "Technology Asset Inventory and Network Map," which would force all regulated entities to:

- Conduct and maintain a written, "detailed inventory" of all technology assets that could impact ePHI confidentiality, integrity, or availability.
- Develop and maintain a "network map" showing the movement of ePHI across systems, including all associated technology assets, software versions, and physical locations.

- Update this network map “at least every 12 months” or after any significant system change.

These are highly complex administrative obligations that would require substantial work to support. Maintaining an ongoing, detailed map of data movement, system updates, and asset tracking is a resource-intensive task that offers little practical benefit for small CEs and their BAs handling limited volumes of ePHI. We call on OCR to ensure that CEs and their BAs are able to implement a reasonable and appropriate approach based on their actual risk exposure. For example, the network map should not require that organizations list every service; instead, listing their use of a cloud service provider—without detailing each service they use within the cloud—should be sufficient for the network map.

Providing Financial Incentives and Support to Strengthen Cybersecurity

CHI urges the HHS to collaborate across its agencies and with other federal partners to develop positive financial incentives that encourage the adoption and maintenance of robust cybersecurity measures. Additionally, CHI recommends the establishment of a new regional extension center (REC)-like program to provide technical assistance and education on cybersecurity best practices.

All CEs will face a degree of financial and operational constraints that hinder their ability to implement comprehensive cybersecurity protections consistent with the proposed rule. Financial incentives can help bridge this gap by enabling small practices to invest in secure IT infrastructure and cybersecurity training. CHI strongly advocates for positive incentives rather than punitive measures, as financial support is more effective in fostering long-term, sustainable improvements. Incentive programs should be structured to enhance both secure data exchange and protection of sensitive patient information, ensuring that small medical practices receive the necessary resources to comply with cybersecurity best practices without compromising patient care.

A successful incentive program would require genuine collaboration across HHS, including the Office for Civil Rights (OCR), the Assistant Secretary for Technology Policy, and the Centers for Medicare & Medicaid Services (CMS). Additionally, cybersecurity-focused federal agencies such as the Department of Homeland Security (DHS) and the Department of Defense (DoD) should be involved to provide expertise and intelligence on emerging cyber threats.
HHS and CMS could incorporate optional cybersecurity-related incentives through existing programs, such as:

- Merit-based Incentive Payment System (MIPS): Introducing cybersecurity as a bonus objective to encourage investment in secure IT systems.
- Medicare Shared Savings Program (MSSP): Offering financial incentives to support cybersecurity improvements in accountable care organizations (ACOs).

- Grants and Direct Subsidies: Providing funding directly to support security risk assessments, corrective action plans, and IT infrastructure modernization.

Importantly, federal funding should flow directly to small providers rather than being absorbed by intermediaries. Direct subsidies and grants should support critical activities, such as replacing outdated IT systems, upgrading cybersecurity defenses, and hiring or contracting cybersecurity professionals. Specifically, federal incentives should help small entities transition to secure, cloud-based electronic health record (EHR) systems and adopt managed IT services that reduce their cybersecurity burden.

In addition to financial incentives, HHS should establish a new REC-like program to provide on-the-ground support for small healthcare providers. The original Regional Extension Center (REC) program, created under the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, successfully helped small practices adopt and optimize EHR systems. A similar program could be designed to:

- Provide technical assistance for small providers struggling to implement cybersecurity best practices.
- Deliver real-time cybersecurity guidance to help practices respond to emerging threats.
- Offer workforce development programs to address the shortage of trained health IT and cybersecurity professionals.

A new REC-like program would be particularly valuable for rural and under-resourced healthcare providers that lack dedicated IT personnel but need support in securing their networks and protecting patient data.

Clarity on Covered Entities' and Business Associates' Roles and Responsibilities

CHI urges OCR to clearly define the roles and responsibilities of CEs and BAs in HIPAA rules to ensure proper cybersecurity accountability. CHI supports OCR clarity on CE and BA roles in:

- Reporting cybersecurity risks, breaches, and mitigation plans;
- Notifying government authorities and affected individuals of a breach;
- Adhering to cybersecurity standards to ensure ePHI protection; and
- Conducting Technology Asset Inventories and Network Mappings.

We support the appropriate distribution of responsibility in the healthcare value chain, which should ensure practical utility and that those with the ability and knowledge for ensuring security updates are incentivized to do so. A notable flaw in OCR's proposal is its fails to accurately represent the roles and responsibilities of cloud service providers: for instance, the proposed rule mandates that each BA, such as cloud service providers, must provide written verification of their implementation of necessary technical controls when it is the responsibility of the customers—namely, HIPAA-covered entities—to configure their cloud services. Shifting the burden to cloud service providers is impractical since the responsibility for configuration rests with the customers.

CHI notes its support for OCR guidance on security updates or providing transition assistance when discontinuing product support; and establishing contingency mechanisms for healthcare entities when a vendor ceases operations or discontinues support for essential IT infrastructure, ensuring access to critical system upgrades.

Recognizing the state-of-the-art security offered by cloud service providers, we request updates to the proposed rule and explanatory text to acknowledge the benefits of cloud adoption for security as well better outline the distinct responsibilities of different HIPAACovered Entities and Business Associates. In describing the different roles of organizations in securing protected health information, we strongly encourage OCR to recognize the distinction between different types of Business Associates, particularly cloud service providers like AWS and other third-party vendors. OCR should take a more nuanced approach that creates distinct frameworks for different categories of Business Associates. Unlike other types of Business Associates, cloud service providers and their customers have distinct roles and responsibilities. For example, cloud service providers are typically responsible for maintaining the physical security and resilience of their infrastructure, such as by restricting physical access to servers and enabling redundant power supplies. Conversely, cloud customers are responsible for their configuration of services and maintaining appropriate security for access credentials. Therefore, OCR should update the rule to align with the cloud shared responsibility model, where infrastructure providers maintain robust security frameworks but do not manage customer security configurations.

Relatedly, the proposed rule would require each Business Associate—including cloud service providers—to provide a written verification that they have deployed the necessary technical controls, such as access controls and other technical procedures. Those configuration decisions are the responsibility of and controlled directly by the customers of cloud service providers. Extending the requirement to all Business Associates, particularly cloud service providers, would be both infeasible and upend the current relationship between cloud service providers and their customers. For example, while AWS can support strong encryption requirements, cloud service providers do not control customer-level encryption decisions. In another example, while cloud service providers can enable backup of data to support resiliency, cloud customers are responsible for configuring the services they receive to enable the backup functionality they seek.

Therefore, we strongly recommend that OCR clarify that it is the cloud service provider's customers' responsibility to configure technical controls on a technology asset hosted by a cloud service provider.

We also seek clarification that a Business Associate (or subcontractor business associate) is not required to deploy a technical control when a Covered Entity (or Business Associate, in the case of a subcontractor) has control over the deployment of a technical control.

Furthermore, several proposed requirements on Business Associates present substantial implementation challenges that may not enhance security outcomes. For example, the blanket requirement for annual security audits should be reconsidered, as many cloud service providers already maintain comprehensive security validations, including SOC2, ISO 27001 certification, and FedRAMP authorization. Relatedly, the requirement for written security control verification every 12 months would generate numerous redundant requests to cloud providers, creating administrative burden without corresponding security benefits. Expanding the volume of documentation to provide specific details about security practices and controls would also increase the attack surface for potential threat actors. OCR should also specify when it may request sensitive security information, how the information will be protected, and how it may be redacted prior to production. The proposed rule also requires Business Associates to (i) terminate workforce members access to "facilities where electronic protected health information or relevant electronic information systems might be accessed" within one hour, and (ii) provide 24-hour notice of a change in or termination of access where a workforce member is or was authorized to access protected health information (PHI) or relevant electronic information systems. These requirements are triggered by unclear standards (e.g., "might be accessed" and "was authorized"), which, without further clarity, would impose onerous reporting and human resource requirements on Business Associates. OCR should provide additional information as to when these post-termination measures are required.

Addressing the diverse roles of Business Associates—and their distinct responsibilities, particularly related to cloud services and other third-party vendors—would add clarity, reduce the implementation burden, and better tailor security practices to each organization to better avert and respond to threats.

Impractical Extensions of Compliance Requirements

OCR's Proposed Rule extends security requirements beyond core health IT systems to include ancillary systems that do not directly interact with ePHI, such as food service and gift shop point-of-sale systems. This broad expansion is impractical and will divert attention and resources away from critical health IT infrastructure. CHI urges OCR to narrow the scope of security requirements to focus on systems directly handling ePHI, rather than loosely connected ancillary systems that do not pose a meaningful cybersecurity risk.

The Need to Encourage Cutting Edge Tools and Services for HIPAA Compliance

It is critical that OCR provide guidance to all CEs and BAs that the use of new secure efficient technologies is fully endorsed, particularly for CEs with resources constraints, As a notable example, the HIPAA Security rules and related guidance should reflect the benefits to security that cloud services provide, as cloud service providers can invest more in state-of-the-art security features that individual HIPAA-covered entities cannot achieve on their own.

Further, CHI fully supports OCR's reliance on encryption of ePHI at rest and in transit as a critical security measure. However, some entities continue to rely on legacy IT systems that lack modern encryption capabilities and cannot easily transition to updated solutions. To address this, OCR should:

- Endorse and recommend that encryption solutions be used in alignment with the latest cryptographic standards, ensuring that practices are not left vulnerable due to outdated vendor technology, while adding an exception for maintaining compensating controls that are adequate to protect against unauthorized access; and
- Expand the emergency exception to include circumstances where time-sensitive access to data is required, rendering encryption impracticable; and
- Offer clear guidance and support for small resource-constrained entities, including those managing legacy systems, including financial assistance or compliance flexibility for transitioning to encrypted systems.

Multi-Factor Authentication (MFA) Implementation Support

CHI supports OCR's support of MFA across all regulated entities' relevant electronic information systems as a critical measure to enhance cybersecurity. The proposed rule acknowledges but does not clarify that CEs and BAs should deploy MFA in a manner consistent with risk analyses. Requiring MFA on all assets that process ePHI will greatly increase burden on clinicians and administrative staff who may utilize several systems over the course of a single patient interaction. To support small and rural entities that face challenges in implementing MFA across all technology assets due to resource constraints and outdated infrastructure. OCR should:

- Allow for phased MFA implementation timelines, particularly for small practices and legacy systems, to prevent disruptions to patient care.
- Adopt a risk-based approach for determining whether MFA should be required or provide CEs and BAs with an exception for systems that need to be accessed in a medical emergency or similar exigency. OCR may also

permit CEs and BAs to expressly allow for risk-based MFA that would trigger when a login presents an unusual risk.

- Provide financial assistance or technical support to small healthcare entities struggling with MFA implementation, ensuring compliance without undue burden.

Timely Patch Management and Vendor Accountability

OCR's proposed standards for timely patch management and compensating controls for unpatchable systems can be improved by encouraging clear timelines and mechanisms for delivering patches to regulated entities and issuing clear guidance on prioritization for security updates, ensuring that healthcare providers can allocate resources effectively to the most critical patches.

Activity Monitoring

OCR suggests that regulated entities should monitor and record all activity in real-time and retain these records. However, this requirement would impose a significant burden on regulated entities due to the vast amount of data generated, without providing a clear advantage for data security. Instead, OCR should allow regulated entities to implement a reasonable and appropriate monitoring and storage system that adequately meets security needs, including specifying the duration for which these records must be retained.

Improving the Offboarding Process

The current rule mandates that access to PHI be terminated within one hour after employment ends, with notification to partners required within 24 hours. We propose aligning this with other sectors by implementing a more flexible standard for access termination and notifications, using the term "promptly" with an established maximum limit. Regulated entities should be allowed some flexibility, as deemed reasonable and appropriate, when circumstances require it.

Creating a Centralized Educational Resource for Cybersecurity Best Practices in Healthcare

CHI recognizes the increasing importance of cybersecurity in safeguarding sensitive patient information, as highlighted in the Proposed Rule. Various federal agencies and partner organizations have developed a range of resources, including the National Institute of Standards and Technology's Cybersecurity Framework 2.0, the HHS 405(d) Program's Health Industry Cybersecurity Practices, the Federal Trade Commission's Start with Security: A Guide for Business, and the HHS Cybersecurity

Performance Goals. While these resources are invaluable, they exist in silos, making it challenging for healthcare entities to access and utilize them effectively. To better serve the healthcare community, we recommend the development of a consolidated, centralized educational resource that compiles these cybersecurity materials into a “one-stop shop.” This resource would provide comprehensive guidelines, best practices, methodologies, and procedures, making it easier for healthcare organizations of all sizes and technical capabilities to reference and implement effective cybersecurity measures.

We urge OCR to take the lead in this initiative by collaborating with relevant federal agencies to create and maintain a consolidated educational resource for cybersecurity best practices. Such a resource will empower healthcare organizations to protect patient data effectively and foster a culture of cybersecurity awareness and compliance within the industry.

Removing the Severability Provision to Align with Statutory Authority

The Proposed Rule’s inclusion of a severability provision exceeds the statutory authority granted to OCR under the HIPAA Security Rule. The HIPAA Security Rule, as authorized by Title II of HIPAA, does not contain a provision for severability, unlike Title I, which is limited to health care access and related matters. The application of severability in Title I is contingent upon a finding of unconstitutionality, which does not apply to the Security Rule. For these reasons, we strongly recommend that OCR withdraw the severability provision proposed in 45 C.F.R. §164.320 of the Proposed Rule. This action will align the rule with the statutory framework of HIPAA and reinforce the agency's commitment to operating within its established legal authority.

IV. Conclusion

CHI appreciates the opportunity to submit comments to OCR and urges its thoughtful consideration of the above input.

Sincerely,

Brian Scarpelli
Executive Director

Chapin Gregor
Policy Counsel

Connected Health Initiative
1401 K St NW (Ste 501)
Washington, DC 20005