799 9th Street NW
Suite 210
Washington, DC 20001

T (202) 354-2600
vizientinc.com

March 7, 2025

Submitted electronically via: www.regulations.gov

The Honorable Anthony Archeval
Acting Director
Office for Civil Rights
U.S. Department of Health and Human Services
Hubert H. Humphrey Building, Room 509F
200 Independence Avenue, SW
Washington, DC 20201

Re: Health Insurance Portability and Accountability Act (HIPAA) Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information (Docket No.: HHS–OCR–0945– AA22)

Dear Acting Director Archeval,

Vizient, Inc. appreciates the opportunity to comment on the proposed rule, Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information (ePHI) (hereinafter "Proposed Rule"). While Vizient appreciates the need to improve cybersecurity of ePHI, we have major concerns that the Proposed Rule will present significant challenges for regulated entities (i.e., covered entities and business associates), including adding excessive costs through unfunded mandates, unrealistic timelines for compliance, and imposing substantial administrative burdens. Additionally, Vizient is concerned that the proposed rigid compliance requirements overlook critical aspects of each regulated entity's resources, circumstances and current approaches to handling security risks. Given these and other concerns detailed below, Vizient urges the Office for Civil Rights (OCR) to reconsider finalizing the Proposed Rule as currently drafted.

Background

Vizient, Inc., the nation's largest provider-driven healthcare performance improvement company, serves more than 65% of the nation's acute care providers, including 97% of the nation's academic medical centers, and more than 35% of the non-acute market. The Vizient contract portfolio represents $140 billion in annual purchasing volume enabling the delivery of cost-effective, high-value care. With its acquisition of Kaufman Hall in 2024, Vizient expanded its advisory services to help providers achieve financial, strategic, clinical and operational excellence. Headquartered in Irving, Texas, Vizient has offices throughout the United States. Learn more at www.vizientinc.com.

Recommendations

While Vizient appreciates the aim to improve cybersecurity of ePHI, we are concerned that several proposed standards and implementation specifications, among other topics, are excessively burdensome or cannot be reasonably implemented within the proposed timeframes.

In addition, given our concerns regarding the burdens associated with the Proposed Rule, as further detailed below, Vizient recommends that OCR work with other government stakeholders to compile existing funding opportunities that are available to support regulated entities' cybersecurity efforts. We also support efforts to make additional funding available to support regulated entities' efforts to comply with the HIPAA Security Rule.

Security Standards: General Rules

Standards and Implementation Specifications

In the Proposed Rule, OCR proposes eliminating the distinction between "addressable" and "required" implementation specifications due to concerns that many regulated entities view "addressable" implementation specifications as optional. Existing regulations include "addressable" implementation specifications, as OCR's goal was to provide greater flexibility for regulated entities to comply with the HIPAA Security Rule.[1] The proposal to require all implementation specifications will add excessive burdens to regulated entities, particularly smaller organizations with fewer resources. Instead of eliminating the distinction between "addressable" and "required", Vizient suggests OCR provide additional education outlining how regulated entities could decide to adopt implementation specifications by using a risk-based approach. For example, a risk-based approach that considers the scale and resources of each entity may help inform compliance decisions while not excessively straining resources.

Environmental Changes

OCR requests feedback on whether the Office's proposals sufficiently clarify that regulated entities are expected to modify their security measures in response to changes in the environment in which health care is provided (e.g., adoption of new technology, evolution of existing technology, and emergence of new threats). Vizient agrees that it is important for regulated entities to be informed when deciding whether to update their security measures as the threat landscape changes. However, regulated entities already face challenges in identifying environmental changes and their response, if any, to such changes may vary for many reasons, including the size of the entity. Further, the Proposed Rule does not provide clarification on how entities are expected to modify their security measures in response to changes in the environment. For example, it is unclear if OCR would expect these changes to happen immediately. If so, this would impose a significant burden on regulated entities. Also, OCR does not provide resources to support these efforts, so Vizient is concerned that regulated entities will continue to struggle to track changes and modify their security measures, even if this point is clarified by OCR. As an alternative, Vizient encourages OCR to release resources that include risk-based prioritization of threats and potential security measures for regulated entities to consider adopting.

Small and Rural Health Care Providers

In the Proposed Rule, OCR requests feedback on whether the proposals adequately consider the needs and capabilities of small and rural health care providers. OCR estimates that the first-

[1] In the 2003 Final Rule, the Department introduced the concept of "addressable" implementation specifications, which it distinguished from "required" implementation specifications. The goal was to provide covered entities with even more flexibility. While none of the implementation specifications were optional, designating some of the implementation specifications as addressable provided each covered entity with the ability to determine whether certain implementation specifications were reasonable and appropriate safeguards for that entity, based on its risk analysis, risk mitigation strategy, previously implemented security measures, and the cost of implementation. However, over time stakeholders asked for removal of the "addressable" designation from the Security Rule because it leads to ambiguity in the rule's application.

year costs associated with the Proposed Rule total approximately $9 billion and for years two through five, estimated annual costs of approximately $6 billion are attributable to recurring compliance activities. Also, OCR states that small and rural health care providers may have needs and capabilities that differ from those of larger regulated entities (e.g., it may be more challenging for these facilities to attract and retain clinicians and security experts to implement strong security measures). Yet, it appears that OCR did not account for these additional challenges that small and rural health care providers may face since the Regulatory Impact Analysis did not include data specific to these types of providers. Vizient reiterates our concerns that small and rural health care providers tend to lack financial and other resources, which does not appear to be adequately considered throughout the Proposed Rule and could lead to even greater challenges for these providers that are unaccounted for by OCR.

Administrative Safeguards

Standard: Technology Asset Inventory

OCR proposes a new standard called Technology Asset Inventory that requires a regulated entity to conduct and maintain an accurate written technology asset inventory and a network map[2] of its relevant electronic information systems and all technology assets that may affect the confidentiality, integrity, or availability of ePHI. The proposed standard is accompanied by three implementation specifications, which provide detail on how to meet the standard for the written technology inventory[3], network map[4] and maintenance.[5] Vizient is concerned that this new standard introduces very broad and burdensome requirements that will cause significant hardships for regulated entities, including increased costs to update and maintain technology and for staff hiring and training. These added responsibilities and consequences may be particularly challenging for small and rural providers to overcome. Considering the wide scope and complexity of the proposed requirements, Vizient suggests OCR instead provide regulated entities with additional resources, including financial assistance, to support their efforts should they decide to create the technology asset inventory standard described in the Proposed Rule.

Standard: Patch Management

OCR proposes a new standard called patch management that requires a regulated entity to implement written policies and procedures for applying patches and updating the configurations of its relevant electronic information systems within a reasonable and appropriate period of time (i.e., within 15 calendar days of identifying the need to address a critical risk and within 30 days to address high-risk vulnerabilities). Effective patch management can involve assessment, tests, and deployment of security patches, which can take variable time and resources. Vizient is concerned the proposed patching timelines of 15 and 30 days for critical and high-risk vulnerabilities are too brief, and potentially unrealistic, given the range of different challenges

[2] A regulated entity's network map would reflect the location of technology assets (e.g., physically located at the regulated entity's worksite, accessed through the cloud).
[3] The proposed written inventory specification requires regulated entities to include technology assets that create, receive, maintain, or transmit ePHI and those that do not but that may affect the confidentiality, integrity, or availability of ePHI. It would also be required to include the identification, version, person accountable for, and location of each of the assets or information system component.
[4] The proposed implementation specification for network map would require a regulated entity to develop a network map that illustrates the movement of ePHI throughout its electronic information systems, including but not limited to how ePHI enters and exits such information systems, and is accessed from outside of such information systems.
[5] The proposed implementation specification for maintenance requires a regulated entity to review and update the written inventory of technology assets and the network map in the following circumstances: (1) on an ongoing basis, but at least once every 12 months; and (2) when there is a change in the regulated entity's environment or operations that may affect ePHI.

that may emerge. Vizient suggests OCR work with providers to identify a more flexible, risk-based approach to address patch management, such as a longer window and financial resources for patch management.

Standard: Workforce Security

OCR proposes clarifications to the Workforce Security standard's implementation specification for termination procedures. Specifically, OCR proposes to require a regulated entity to establish and implement written procedures for notifying another regulated entity when there is a change in or termination of a workforce member's authorization to access ePHI or relevant electronic information. Specifically, regulated entities would be required to provide this notice to other regulated entities as soon as possible, but no later than 24 hours after the change in the workforce member's authorization to access ePHI or relevant electronic information systems. Additionally, OCR proposes to require that a workforce member's access to ePHI and relevant electronic information systems be terminated as soon as possible, but no later than one hour after the workforce member's employment or other arrangement ends. Vizient is concerned that these strict notification and termination of access requirements are impractical, particularly for entities with complex systems or large workforces who access numerous networks and relevant electronic information systems. While Vizient agrees that addressing workforce security issues are important, if finalized, Vizient suggests adopting a more feasible timeframe for such notifications and access changes, such as over a series of business days, as it balances both organizational security and operational feasibility of the regulated entities.

Standard: Contingency Plan

OCR proposes to modify the current implementation specification for disaster recovery planning by clarifying that a regulated entity is required to establish, and implement, as needed, written procedures to restore both its critical relevant electronic information systems and data within 72 hours of a breach. The proposed requirement to restore all critical systems within 72 hours after a data breach does not reflect operational realities, particularly for complex organizations with interconnected systems, where more time is needed for restoration. Should OCR finalize the Proposed Rule despite our concerns, Vizient urges OCR to allow regulated entities to employ a more flexible, risk-based approach to contingency planning.

Standard: Business Associate Contracts and Other Arrangements

To avoid leaving a gap in protections from risks to ePHI related to regulated entities' vendors and supply chains[6], OCR proposes a new implementation specification for a regulated entity to obtain written verification from its business associates that they have deployed these technical safeguards. While the existing requirement for written satisfactory assurances provide a framework for compliance, the new proposed verification requirements could introduce significant and unnecessary administrative burdens without ensuring a corresponding security benefit. Further, regulated entities often have a large volume of business associate contracts and other agreements so OCR may not be grasping the significance of this administrative burden. Vizient urges OCR to retain the current model of contractual assurances.

[6] The current HIPAA Security Rule requires a regulated entity to obtain written satisfactory assurances that its business associate is complying with the appropriate technical safeguards regarding ePHI before allowing the BA to create, maintain, receive or transmit ePHI on its behalf.[6] However, the Security Rule does not require a verification that regulated entities are taking the necessary steps to protect such ePHI.

Technical Safeguards

Standard: Encryption and Decryption

OCR proposes a new implementation specification requirement for a regulated entity to configure and implement technical controls to encrypt and decrypt all ePHI it maintains, with limited exceptions[7]. Under the proposal, a regulated entity would need to ensure that an encryption solution it adopts meets prevailing cryptographic standards, which are not defined in the Proposed Rule's regulatory text, prior to using it. Mandating encryption for all electronic information systems without broader exceptions does not consider the financial, technological and resource limitations of regulated entities. Vizient urges OCR to work with regulated entities to get a better understanding of the challenges associated with limited exceptions and why expanded exceptions may be necessary for smaller providers or specialized use cases where full compliance is impractical.

Standard: Configuration Management

OCR proposes a new standard for configuration management requiring a regulated entity to establish and deploy technical controls for securing relevant electronic information systems and technology assets in a consistent manner. The Office proposes five implementation specifications for this proposed standard, including one for anti-malware protection where a regulated entity would be required to deploy technical controls that protect all the technological assets in its relevant electronic information systems against malicious software. When determining how to fulfill this proposed obligation, OCR offers suggestions for technical controls but also asks for feedback on whether regulated entities should be required to deploy an endpoint detection and response (EDR) and security information and event management (SIEM) as technical controls. Vizient suggests OCR consider an approach where the use of technical controls, including EDR and SIEM solutions, are optional. OCR should encourage organizations to take a risk-based approach to determining which technical controls to utilize rather than rather than a one-size-fits-all approach.

Standard: Authentication

OCR proposes an implementation specification to require a regulated entity to deploy Multi-Factor Authentication (MFA). Specifically, OCR proposes a requirement for a regulated entity to deploy MFA to all technology assets in its relevant electronic information systems to verify that the person seeking access to its relevant electronic information system is the user that the person claims to be. Further, OCR indicates that a regulated entity should deploy MFA to all technology assets in its relevant electronic information systems in a manner consistent with its risk analysis. The Proposed Rule does allow for limited exceptions to this requirement, but the Office imposes strict conditions that must be met for the exemption to apply. Vizient believes that while the use of MFA can increase security against unauthorized access to ePHI by adding additional layers of protection, requiring enterprise-wide MFA without reasonable exceptions creates undue hardship for regulated entities.

[7] For example, adoption of health IT that is certified through the ONC Health IT Certification Program as having the technical capability to encrypt, or prevent the local storage of, electronic health information stored on end-user devices after use of the technology on those devices stops may contribute to a regulated entity's compliance with the proposed implementation specification for encryption and decryption. See 45 CFR 170.315(d)(7)

Organizational Requirements

Standard: Business Associate Contracts or Other Arrangements

OCR proposes to add a new implementation specification requiring a business associate agreement to include a provision requiring a business associate to report to the covered entity activation of its contingency plan without unreasonable delay[8], but no later than 24 hours after activation.[9] The mandate for business associates to notify covered entities upon contingency plan activation within the proposed 24-hour timeframe is vague and will lead to confusion about the specific situations it is intended to address. Furthermore, requiring updates to such contracts or other arrangements represents a substantial effort that will take additional time and resources from already strained providers. Vizient suggests OCR work with regulated entities to discuss more practical approaches, such as a risk-based approach, to provide proper notice of security incidents, rather than more rigid requirements that are associated with administrative burden.

Transition Provisions

OCR states in the Proposed Rule that regulated entities may be concerned with the anticipated administrative burden and cost of revising their business associate agreements to comply with the substantial number of new requirements of the revised Security Rule. As a result, OCR proposes to allow regulated entities to continue to operate under certain existing business associate agreements or other written arrangements until the earlier date of: (1) the date such contract or other arrangement either is renewed on or after the compliance date of the final rule; or (2) a year after the effective date of the final rule. Vizient notes that the number of contracts between covered entities and business associates could be in the thousands, and updating this number of contracts can be a lengthy process, requiring significant time, effort and cost. Because of this, covered entities and business associates will need to dedicate significant time and resources to ensure compliance with these requirements. As such, should the Proposed Rule be finalized despite our concerns, Vizient urges OCR to extend the timeline to update business associate agreements or other written arrangements.

Recurring Requirements

The Proposed Rule adds a significant number of new requirements to the HIPAA Security Rule and, for several of the new requirements they must be reviewed and potentially updated at a regular interval; most commonly once every 12-months. Vizient notes that given the differing levels of risk across a regulated entity's areas of operations, implementing a strict cycle to review and update policies and procedures would require a considerable effort to gather the necessary information and make the required changes without significantly improving security. To reduce administrative burden, Vizient suggests OCR clarify that regulated entities can establish their own risk-based review schedule.

New and Emerging Technologies Request for Information

The Proposed Rule requests information on how the HIPAA Security Rule protects ePHI used in

[8] This proposal would align with the enhanced Cybersecurity Performance Goals (CPG) for Third Party Incident Reporting because this proposal would require a business associate to both report to a covered entity or another business associate activation of its contingency plan within 24 hours of such activation and report known or suspected security incidents.

[9] The proposed requirement to provide notice without unreasonable delay, but no later than 24 hours after a contingency plan is activated, would also apply when a business associate that is a governmental entity enters into an arrangement with a covered entity that is also a governmental entity and also when a business associate enters into a business associate agreement with a subcontractor.

new and developing technologies, including any benefits, drawbacks, or unintended consequences. One circumstance that Vizient encourages OCR to consider is where ePHI is housed outside the United States. Many providers want protected data to be stored in the United States. However, some companies may store data abroad to reduce costs. Vizient recommends OCR gather more insights on how to protect ePHI from emerging threats and security gaps from new and developing technologies where data is not stored domestically.

Conclusion

Vizient membership includes a wide variety of hospitals ranging from independent, community-based hospitals to large, integrated health care systems that serve acute and non-acute care needs. Additionally, many hospitals are specialized, including academic medical centers and pediatric facilities. Individually, our members are integral partners in their local communities, and many are ranked among the nation's top health care providers. In closing, on behalf of Vizient, I would like to thank HHS for the opportunity to share feedback on this important Proposed Rule. Please feel free to contact me, or Randi Gold at Randi.Gold@vizientinc.com, if you have any questions or if Vizient may provide any assistance as you consider these recommendations.

Respectfully submitted,

Shoshana Krilow
Senior Vice President of Public Policy and Government Relations
Vizient, Inc.