Ascension

Lisa J. Pino, JD
Director
Office for Civil Rights
Attention: HITECH Act Recognized Security Practices Request for Information
RIN 0945-AA04
200 Independence Avenue SW
Washington, DC 20201

June 6, 2022

Submitted electronically to: http://www.regulations.gov

RE: HITECH Act Recognized Security Practices Request for Information (RIN 0945-AA04)

Dear Director Pino:

Ascension appreciates the opportunity to submit comments in response to the request for information (RFI) entitled *Considerations for Implementing the Health Information Technology for Economic and Clinical Health (HITECH) Act, as Amended*.[1]

Ascension is a faith-based healthcare organization dedicated to transformation through innovation across the continuum of care. As one of the leading non-profit and Catholic health systems in the U.S., Ascension is committed to delivering compassionate, personalized care to all, with special attention to persons living in poverty and those most vulnerable. In FY2021, Ascension provided $2.3 billion in care of persons living in poverty and other community benefit programs. Ascension includes more than 150,000 associates and 40,000 aligned providers. The national health system operates more than 2,600 sites of care – including 143 hospitals and more than 40 senior living facilities – in 19 states and the District of Columbia.

Ascension is strongly committed to both compliance and innovation which, combined with our experience as a microcosm of the healthcare system, informs the following responses to the questions raised by the Office for Civil Rights (OCR). We appreciate OCR's engagement on these important issues and policy questions, and look forward to working with OCR on implementation of the HITECH Act, as amended. We also echo comments offered by the Confidentiality Coalition, of which Ascension is a member, which note that while enforcement action remains an essential tool for deterrence, and regulated entities with lax privacy and security practices should face appropriate penalties, OCR should, to the maximum extent possible, implement the HITECH Act in a manner that encourages compliance, cooperation and coordination in the face of common threats, and directs OCR resources to supporting and advancing these goals.

[1] 87 Fed. Reg. 19833 (April 6, 2022).

Section 13412 of the HITECH Act, as Amended

As OCR explains, Public Law 116-321 amends Part 1 of subtitle D of the HITECH Act to require OCR to consider recognized security practices that organizations adequately demonstrate were in place for the previous 12 months when determining penalties. The Department of Health and Human Services (HHS), through OCR, seeks input regarding stakeholders' voluntary implementation of recognized security practices. Additionally, HHS seeks input on any additional information or clarifications that regulated entities currently need from OCR regarding the agency's planned implementation of the new law. Specifically, OCR solicits input on recognized security practices that regulated entities have implemented or plan to implement. Ascension has found the appointment of a Chief Information Security Officer (CISO), who is tasked with leading a department of cybersecurity, governance, risk and compliance (GRC) associates in coordination with several managed security services providers, is a key recognized security practice. The CISO's department provides its regulated entities with a comprehensive set of security and privacy services in accordance with Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations and cybersecurity best practices.

Additional security controls that we have successfully implemented to date include, but are not limited to: vulnerability management, security information and event management (SIEM) and security orchestration, automation and response (SOAR), identity and access management (including multi-factor authentication), cyber insurance, data protection, remote access, third party security, cloud security, development, security, and operations (DevSecOps)/application security, privileged access management, medical device and operational technology security, firewalls and other network security, endpoint protection and encryption, utilization of 24/7 security operations center, penetration testing, security incident response and case management, email and collaboration suite security, and disaster recovery. We also plan to implement a significant amount of investment and resources around "zero trust"-type controls, security event and orchestration automation, and more robust and resilient backups.

OCR further solicits input regarding standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the National Institute of Standards and Technology (NIST) Act, and whether regulated entities rely on these when establishing and implementing recognized security practices. Ascension does rely on the NIST framework and guidance documents to define, develop, and manage its cybersecurity and governance, risk, and compliance programs. We, as regulated entities, must also engage external, third-party auditing firms to use the NIST framework when performing maturity or risk assessments. And when developing policies, standards, and guidelines, we consult NIST documentation for relevant guidance and best practice. Other frameworks may be used to supplement different business requirements, such as the Open Web Application Security Project® (OWASP) framework for application security, the Center for Internet Security (CIS) framework for cloud security, the Payment Card Industry Data Security Standard (PCI-DSS) for payment card environments, the Control Objectives for Information and Related Technologies (COBIT) framework, and the American Institute of Certified Public Accountants (AICPA) cybersecurity risk management reporting framework.

Additionally, OCR solicits input on which approaches promulgated under section 405(d) of the Cybersecurity Act of 2015 regulated entities rely on when establishing and implementing recognized security practices. As a regulated entity, Ascension participates in the development of best practices and other initiatives for 405(d) through CISO representation on the Healthcare and Public Health Sector Coordinating Council (HSCC) Cybersecurity Working Group (CWG), which is coordinated through the Health Sector Council (https://HealthSectorCouncil.org). We also use best practices documentation produced by the HSCC CWG to guide development of security controls and capabilities. We rely

exclusively on the NIST Framework (and guidelines), HIPAA regulations, and HITECH, however, we leverage other control frameworks such as COBIT and AICPA, as discussed above.

OCR solicits input on the steps covered entities take to ensure that recognized security practices are "in place." In Ascension's experience, there are three primary ways in which security practices are ensured to be "in place": (1) establishing clear policies, guidelines, and standards, based on the NIST framework, that serve as administrative controls and set the expectations for technology throughout its lifecycle; (2) utilizing automated, technology-driven monitoring to detect areas of non-compliance or cybersecurity risk, which includes things such as vulnerability scanners, web and network based firewalls, endpoint detection and response, SIEM tools, cloud compliance suites, email monitoring and protection, and data loss prevention; and (3) internal and third party audits, which may range from assessment of specific areas of risk (*e.g.*, patch management) to overall program evaluation (*e.g.*, cybersecurity program maturity assessments).

While implementation of recognized security practices may, to a degree, vary across the enterprise, given the size and scope of the health system, best practice has been to ensure they are generally established in coordination with the service or application being deployed. This ensures that, once the standard or secure configuration is identified and implemented, all similar technologies should align with the standard with very few exceptions. Additionally, Ascension establishes Key Performance Indicators (KPIs) and reporting metrics to monitor adherence to security practices whenever possible.

Finally the Department requests comment on any additional issues or information the Department should consider in developing guidance or a proposed regulation regarding the consideration of recognized security practices. To that end, as discussed herein, Ascension relies on the NIST framework as the cornerstone of its program. We believe careful curation, organization, and presentation of NIST cybersecurity documents, tools, and publications would help regulated entities ensure that critical resources otherwise devoted to researching and digesting such documents are most efficiently leveraged.

Section 13410(c)(3) of the HITECH Act

OCR notes that Section 13410(c)(3) of the HITECH Act requires the Department to establish a methodology whereby an individual who is harmed by noncompliance with the HIPAA Rules may receive a percentage of a penalty or monetary settlement collected with respect to that noncompliance. Although the Enforcement Rule permits the Department to consider certain types of harm when determining the amount of a penalty, neither the HITECH Act nor the HIPAA Rules define harm generally or for the purpose of identifying and quantifying harm to determine an amount to be shared with an individual. For this reason, the Department seeks input about how to define harm and what bases should be used for deciding which injuries are compensable.

As a threshold question, OCR invites input on what constitutes compensable harm with respect to violations of the HIPAA Rules, including–among other clarifying questions–whether only economic harm should be considered, whether harm should be limited to the types of harm identified as aggravating factors in assessing CMPs, and whether the potential for future harm should be compensable. While there is no question that individuals may suffer both economic and noneconomic harms as a result of HIPAA violations, we agree with comments offered by the Confidentiality Coalition that this reality does not in turn mean that all such harms should be compensable *through the mechanism contemplated in*

Section 13410(c)(3) of the HITECH Act. We thus encourage OCR to exclude noneconomic harms from compensable harm, as this concept will be exceedingly difficult to determine and many of the noneconomic harms (*e.g.*, emotional frustration or annoyance) can ultimately derive from a multitude of factors and experiences, making it difficult to prove or disprove the direct relationship with an actual violation incident and creating significant increased litigation burden on all parties–acknowledging, however, that individuals continue to retain other avenues for appropriate recovery, as noted below.

We also encourage OCR to consider policies that reasonably account for the facts and circumstances of applicable violations, as actual harm from a breach or violation may or may not uniformly impact all individuals affected by even the same incident. As a hypothetical example, in an inappropriate access case, one record may have only been accessed for five seconds while searching for another record that actually had information taken from it, but we would likely notify both individuals; this would not amount to the same harm or impact with respect to the respective patients' compromised information and OCR policy should thus account for this differential impact by refraining from treating all individuals "harmed" by a violation in a uniform manner.

We further recommend that harm include only financial harm that can be clearly demonstrated by the impacted individual and not include future harms in situations where there is no existing, demonstrable or tangible evidence for the alleged future harm. A patient's ability to recover for harm should also take into account whether the individual has utilized follow-on protective measures offered in response to a breach, such as credit monitoring, and whether an individual's decision to not engage in such protective measures was a demonstrable cause of harm in question to the individual. We also encourage OCR to exclude from the definition of harm any damages that an individual can otherwise recover through other available mechanisms, such as a civil lawsuit or insurance coverage. Types of harm that are already compensated for through other mechanisms should not be considered for purposes of receiving a portion of a civil money penalty (CMP) settlement.

Additionally, OCR solicits input on whether harm should be presumed in certain circumstances and outlines several additional clarifying questions. We encourage OCR to avoid adopting a standard by which harm is presumed in any circumstance. While regulated entities may violate the HIPAA Privacy and Security Rules in a manner that results in an enforcement action for appropriate reasons, not all violations result in harm to individuals. In Ascension's experience and observations, one of the most noticed and significant harms to a patient impacted by privacy violations tends to be identity theft, which is increasingly common and thus hard to prove direct relationship to a specific incident.

We encourage OCR to instead require that impacted individual(s) produce evidence of harm as an appropriate precaution against frivolous complaints and resulting unnecessary resource diversion. Furthermore, this approach would align with other class action privacy lawsuits, in which harm/financial harm typically needs to be proven by an individual to recover damages, unless a known or demonstrable negative impact has occurred. Finally, admissible evidence should demonstrate a direct link between the behavior that the CMP is arising out of and the financial harm that the individual experienced; there should be no room for reasonable doubt that the person suffered the financial harm based on a different violation or action (*e.g.*, an unsecured online credit card transaction).

The Department also seeks information about current real-world impacts of loss of privacy on an individual's willingness to seek care or disclose health information to covered entities to better understand the nature of privacy harms that occur. As a large, national health system, Ascension has observed directly and indirectly the potential impacts of varying degrees of privacy loss. We also

frequently engage healthcare consumers regarding their care needs, preferences, and concerns. To date, we have not experienced any significant degree of individuals refusing to seek care because of potential privacy impact.

The RFI solicits input on whether the Department should recognize as harm the release of information about a person other than the individual who is the subject of the information (*e.g.,* a family member whose information was included in the individual's record as family health history) for purposes of sharing part of a CMP or monetary settlement. While we reiterate the recommendation that harm for these purposes be limited to demonstrable financial harm, if harm were more broadly defined, we would encourage OCR to limit the scope of harm to only those individuals whose records were subject to a violation (and for whom harm has been established), given the potential for unintended downstream impacts such as a chilling factor on patient willingness to share important—and often deidentified—family history with their treating clinician.

OCR further asks whether the Department should consider external recoveries or compensation received, available, or likely to be available for harmed individuals when deciding whether to set aside funds for distribution. We strongly encourage OCR to take these factors (*e.g.,* civil lawsuits) into consideration. Similarly, in subsequent questions, OCR asks whether the distribution methodology should adjust or deny distribution amounts based on the potential or actual compensation of individuals through other mechanisms outside of the distribution requirement for the same action under the HITECH Act, such as in a manner similar to the Consumer Financial Protection Bureau. For the reasons articulated herein, we encourage OCR to ensure the distribution methodology also takes these factors into account, as individuals should certainly be made whole for violations resulting in harm, but should not have the ability to recover inappropriately beyond that. At the same time, the distribution methodology should recognize and account for in-kind benefits (*e.g.*, credit monitoring paid for by the entity) as compensation for purposes of determining the appropriate distribution to be made.

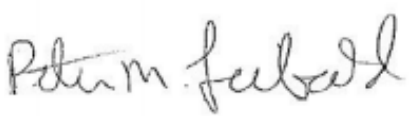
OCR also solicits input on several questions regarding how covered entities should provide notice to affected individuals that monetary distribution may be available. With respect to an individual who is deceased, we note that most violations of the privacy rule would result in no harm to the family or no otherwise unknown harm to the individual's estate, thus it would not be appropriate for entities to be required to notify the family or estate—or for those not directly harmed to be eligible to receive a distribution. Furthermore, if an individual cannot be located and notified within the time frame for distribution, we believe notification and eligibility should be handled in a manner similar to class action lawsuits (e.g., time limited) and the individual should not be permitted to receive a distribution at a later date if they were not able to be located and notified despite appropriate efforts.

Finally, the RFI solicits input on goals that the Department should prioritize when selecting a distribution model; for example, whether OCR should maximize distributions of available funds to the individuals most harmed by noncompliance. As noted above, not all individuals are impacted equally by even a common single violation. However, determinations regarding which individuals have been "most" impacted could be very difficult for the covered entity to be able to quantify if this requirement were to fall on them. We also caution OCR that categorizing some information as "more" damaging if released (e.g., mental health or substance use disorder information), and increasing financial recovery based on the type of healthcare information released could perpetuate negative stigmas around certain diagnoses, despite ongoing efforts to overcome these stigmas. We thus caution OCR to fully consider the potential implications—immediate and downstream—of any distribution model proposed.

Conclusion

We appreciate your consideration of these comments. If you have any questions, or if there is any additional information we can provide, please contact Mark Hayes, Senior Vice President for Policy and Advocacy for Ascension, at 202-898-4683 or mark.hayes@ascension.org.

Sincerely,



Peter M. Leibold
Executive Vice President and Chief Advocacy Officer
Ascension