American Health Information Management Association®

233 N. Michigan Ave., 21st Fl., Chicago, IL USA 60601-5809 | www.ahima.org | 312.233.1100

May 23, 2022

Director Lisa J. Pino
Office for Civil Rights
US Department of Health and Human Services
200 Independence Avenue, SW
Room 509-F, HHH Building
Washington, DC 20201

RE: *Considerations for Implementing the Health Information Technology for Economic and Clinical Health (HITECH) Act, as Amended*

Submitted electronically via www.regulations.gov

Dear Director Pino,

On behalf of the American Health Information Management Association (AHIMA), I am responding to the Department of Health and Human Services (OCR) Office for Civil Rights (OCR) *Considerations for Implementing the Health Information Technology for Economic and Clinical Health (HITECH) Act, as Amended* Request for Information (RFI).

AHIMA is a global nonprofit association of health information (HI) professionals. AHIMA represents professionals who work with health data for more than one billion patient visits each year. The AHIMA mission of empowering people to impact health drives our members and credentialed HI professionals to ensure that health information is accurate, complete, and available to patients and clinicians. Our leaders work at the intersection of healthcare, technology, and business, and are found in data integrity and information privacy job functions worldwide.

Following are our comments and recommendations on selected sections of the RFI.

Public Law 116–321 (Section 13412 of the HITECH Act, as Amended)

What recognized security practices have regulated entities implemented? If not currently implemented, what recognized security practices do regulated entities plan to implement?

AHIMA recommends OCR recognize the HHS 405(d) Workgroup's Health Industry Cyber Practices (HICP): Managing Threats and Protecting Patients[1] product as a best practice resource eligible under this program for recognition. "The 405(d) program is a collaborative effort between industry and the federal government to align

[1] https://405d.hhs.gov/Documents/HICP-Main-508.pdf

healthcare industry security practices in an effort to develop consensus-based guidelines, practices, and methodologies to strengthen the healthcare and public health (HPH) sector's cybersecurity posture against cyber threats[2]." With the 405(d) program and the HICP being both joint efforts between the federal government and industry, they represent a diverse range of inputs and are demonstrative of an industry best practice that fit the needs of all providers. Additionally, by adopting a publicly developed industry best practice there will be no cost burden passed on to providers given that the HICP is freely available. By ensuring that the recognized security best practice is low or no cost, greater adoption and participation in the program can be expected. The end goal of this program is to make healthcare safer by incentivizing providers to adopt security best practices. AHIMA believes the adoption and recognition of the 405(d) HICP accomplishes both goals.

If OCR elects to recognize multiple sets of best practices, or provides several recommendations, AHIMA also recommends OCR include the HITRUST Certification of the NIST Cybersecurity Framework[3]. The HITRUST program includes a robust certification, quality assurance and recertification process ensuring organizations utilizing HITRUST are actively engaged in securing their networks. Similar to the 405(d) program HICP mentioned above, HITRUST is publicly available and a tool that enables access to best practices for even the smallest covered entities. Multiple organizations also currently engage in the HITRUST certification process and thus would be eligible for this OCR program with little to no additional burden placed on the provider beyond the burden of implementing HITRUST itself.

Finally, we recommend OCR conduct a landscape review of individual state level system security plan requirements and best practices mandated by state law that exceed the minimum requirements under the HIPAA Security Rule. Ensuring that state level cybersecurity best practice requirements remain in scope for consideration under this program helps limit the compliance burden placed on small, covered entity providers. These state level requirements could also be used by OCR as a means to increase participation in a cybersecurity best practices program that will keep both a patient's information and covered entities themselves more cyber secure.

What constitutes implementation throughout the enterprise (e.g., servers, workstations, mobile devices, medical devices, apps, application programming interfaces (APIs))?

AHIMA supports the continued development and further understanding of when a cybersecurity best practice is considered implemented and when covered entities become eligible for participation in the best practices process. Determining when a best practice is implemented presents a unique challenge for OCR at this time, as implementation will be dictated depending on what best practice a covered entity specifically implements. While most best practices will follow a similar structure and implementation procedures, no two best practices will be identical. As a result, AHIMA recommends OCR propose, as part of an NPRM process, a series of best practices that could conform with the requirements outlined under PL 116-321 and define what implementation should consist of through a proposed rule. By specifically outlining what implementation should consist of, covered entities have a specific set of requirements to work towards.

Ensuring the active and consistent use of security best practices is easier for OCR to ensure than determining what implementation means. Covered entities, as part of their best practices, must routinely review, test, and confirm the implementation of these best practices. AHIMA recommends OCR adopt a policy requiring covered entities to review their security stature and best practices not more than annually and to document these internal reviews. This policy should also align with requirements already imposed under the HIPAA Security Rule and not create a duplicative burdensome reporting structure on covered entities. By limiting the requirement to no more than annually, OCR ensures covered entities would not assume additional burden beyond what is already dictated by the cybersecurity best practices themselves.

[2] https://405d.hhs.gov/about
[3] https://hitrustalliance.net/certification/nist-cybersecurity-framework-certification/

If OCR were looking for additional opportunities to verify implementation and use of these best practices, the Security Risk Assessment (SRA) Tool[4] could be utilized. Mandatory risk assessments are already required under the HIPAA Security Rule. Utilizing the SRA Tool would align OCR with other work taking place within HHS and would ensure duplicative requirements are not being placed upon covered entities. Additionally, AHIMA encourages OCR to review and utilize the available certifications such as HITRUST as another avenue for verifying that these best practices are in place and being utilized.

AHIMA does caution OCR that as part of these activities, it is crucial that verifying implementation and use of security best practices does not duplicate existing federal requirements. As stated above for instance, covered entities are already required to conduct regular risk assessments under the HIPAA Security Rule. It is crucial for OCR to ensure that reporting requirements are not duplicated and that attestation to having these best practices in place does not create additional reporting burden. Additional burden only increases the likelihood under resourced providers will not be able to participate in the program or that a provider may choose not to participate, leaving them more vulnerable to cyberattack and intrusion.

Finally, AHIMA recommends OCR consider an implementation and execution requirement process that provides flexibility for covered entities depending on the size of their practice. The baseline for implementation and execution will vary across the health system and the minimum compliance and implementation level for a small, covered entity will be much different than it will be for a large, covered entity. As such, OCR should take the differences in size into consideration when determining what the baseline requirements for implementation are for covered entities.

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.

AHIMA recommends OCR proceed to a notice of proposed rulemaking (NPRM) following the conclusion of this RFI. By moving to an NPRM, instead of implementing guidance on how best to give covered entities relief when following cybersecurity best practices, covered entities can prepare accordingly for the implementation of this program. By allowing covered entities to prepare, OCR will see an increase in adoption of cybersecurity best practices and education can be provided to assist covered entities in making their systems secure. Moving forward with a guidance only process will significantly stunt the adoption of this program as many covered entities will be unaware of its existence or will lack the knowledge necessary to comply. It is in OCR and the nation's best interests to ensure as many providers as possible participate in this process and implement robust OCR recognized best practices.

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

What Constitutes Compensable Harm with Respect to Violations of the HIPAA Rules?

AHIMA urges OCR to move beyond linking civil monetary penalties (CMPs) and their payment entirely to a determination of if harm took place within a harm standard. We recommend OCR review counter proposals to this process such as the one moved forward from the Confidentiality Coalition on how to determine who qualifies for a CMP[5]. Current HHS policy related to CMPs and HIPAA related breaches has moved away from the harm standard and the need to demonstrate harm. Linking the payment of CMPs to patient harm would be a reversal of existing HHS policies and would make enforcement of CMPs and the payment of CMPs incongruous. Additionally, it remains difficult to define harm to a patient due to the number of data breaches that happen daily, including those within and outside of the healthcare industry. There is no widely accepted industry standard to define

[4] https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool
[5] https://www.confidentialitycoalition.org/wp-content/uploads/2022/02/Chart-of-Potential-HIPAA-Penalty-Distribution-Methodologies-Chart-A.pdf

either economic harm or non-economic harm. Furthermore, determining if a health data breach from a covered entity resulted in harm directly to a patient would be difficult. Without knowing if direct harm took place, assigning a CMP to that potential harm would be extremely difficult. As a result, AHIMA recommends OCR move away from linking CMP payments to patients solely to a harm standard and recommend OCR propose a new process for determining whether a breach impacts a patient and take into consideration harm and other factors.

Should the potential or future harm be compensable?

AHIMA recommends against utilizing harm as a standard for determining CMPs under the HIPAA Rules. Harm continues to be an outdated standard no longer utilized by OCR for determining the impact of a breach on a patient. Without a clear definition of harm and a proposal from OCR related to defining breach impact, it is difficult to measure harm. This is especially true given that under the current HIPAA rules it is difficult to determine the type of disclosure and how those disclosure types impact the harm standard.

If OCR were to continue with utilizing a harm standard for CMPs, AHIMA recommends against making future harm compensable. Currently there is no federal standard in healthcare related to measuring future harm and it could be difficult to prove a patient suffered actual harm and that it was proximately caused by one specific breach. With so many unknown variables related to both defining future harm and measuring it, future harm will not be a viable solution for compensating patients impacted by a breach.

Finally, AHIMA recommends that if OCR were to move forward with a future harm CMP payment process for patients, OCR should consider as a mitigating factor whether impacted patients were provided by the covered entity with services such as credit monitoring. Allowing for such mitigating circumstances could allow OCR to give credit to the covered entity who works to protect a patient potentially impacted by a breach from future harm, thereby limiting the amount of the penalty or monetary settlement as a result of noncompliance.

Should OCR allow individuals to include actual and perceived harm?

AHIMA recommends OCR move away from implementing a CMP policy related to perceived harm. OCR should work to make the requirements as clear as possible and to ensure it establishes a clear bright line removing ambiguity as it relates to harm. Under a harm standard, OCR should indicate the factors involved in whether harm did or did not happen. Opening the door to including perceived harm creates the ability for all breaches to be under consideration for a CMP payment, when the reality is much murkier. By creating an actual harm standard OCR ensures the rules and requirements are clear and easily understandable by all parties involved.

If OCR were to move forward with a perceived harm standard for repayment of CMPs, then it is crucial for OCR to establish clear time requirements for when a harm must be perceived. Perceived future harm could be assumed indefinitely by some patients and that leaves the covered entity exposed to long-term risk, including reputational harm, even if the chance of future perceived harm is low.

Should harm be presumed in certain circumstances?

AHIMA recommends OCR maintain alignment and consistency with the existing HIPAA Privacy and Security rules which require evaluation of compliance by a covered entity. Individuals who are harmed by a covered entity should have the burden of proof placed upon them and should be required to provide credible evidence of the harm they have endured. The harmed individuals should also provide objective, specific, and concrete evidence demonstrating that injury was the result of a specific breach of a covered entity and not the result of a superseding event. As part of these recommendations, AHIMA also urges OCR to move forward with an NPRM that provides specific requirements related to the types of evidence that must be provided by an individual to demonstrate harm.

Finally, AHIMA supports a process in which OCR presumes harm only in instances where willful neglect has been demonstrated by a covered entity and that that entity failed to take corrective action within 30 days. Both circumstances would need to be proven through a robust investigation process. Willful neglect and the failure to take corrective action would be a clear circumstance where OCR is able prove that a covered entity was conscious and intentionally failed or was recklessly indifferent and failed to take corrective action.[6] By doing so OCR would fulfill the burden of showing when a presumed harm could be compensable with a CMP payment to an impacted individual.

Should the Department 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 settlements?

AHIMA recommends OCR not pursue a process of adjudicating CMPs for third party harm from disclosure. At this time it would be too difficult to fully quantify how a third party is harmed from a breach of information. This is especially true given that the HIPAA rules currently define data contained within a patient's record that includes information from a third party – such as familial medical history – belongs to the individual patient not the third party. Such occurrences are particularly common when involving maternal infant records, where often information related to the mother is incorporated into the infant's record or vice versa. Providing CMPs to a third party because of a breach of that data would lead the CMP payment process to be incongruous with the already in place HIPAA penalties. The current state of health IT only serves to make that process even more difficult. Current technology often does not allow for the segmentation of data and thus could create confusion and increase burden on both the provider and OCR in determining third party breach. This fact with potential incongruous policies creates a landscape difficult for OCR to consistently payout CMPs.

Should there be a minimum total settlement or penalty amount before the Department sets aside funds for distribution?

AHIMA recommends OCR undergo a process to conduct a literature review of relevant legal texts and previous related breach of data settlements within the health sector to determine a process for CMP distribution and settlement. Once this literature review is completed, AHIMA recommends OCR conduct an NPRM that outlines the requirements for payment and the process for determining the percentage of CMPs to patients impacted by a HIPAA breach.

How should harmed individuals be identified? How should they be notified that they may be eligible for distributions?

AHIMA recommends OCR mirror the breach notification requirements for providing notice to impacted patients of their right to a HIPAA related settlement. By following similar federal policies that are already in place, OCR ensures there will be less regulatory burden and duplicity placed on covered entities and those involved in the breach and CMP process.

What goals should the Department prioritize when selecting a distribution model?

AHIMA recommends OCR propose limits related to the CMP payments eligible to impacted patients for each type of harm to ensure that each harm payment is congruous across all decisions. By ensuring that the type of harm suffered is reimbursed at a standard level, OCR sets clear federal requirements that are easily understood by all parties involved in the process.

[6] 45 CFR 160.401.

Finally, the Department requests comment on any additional factors or information the Department should consider in developing a proposed methodology to share a percentage of CMPs and monetary settlements with harmed individuals.

AHIMA urges OCR to remember in this process that while an impacted patient is a victim of a data breach, a covered entity may also be a victim of cybercrime at the same time. In this RFI, OCR already indicates that covered entities may follow a set of cybersecurity best practices and still fall victim to cybercrime through no fault of their own. Knowing this, we urge OCR to impose a process by which CMPs are paid – when appropriate – by the entities committing the cybercrime. Cybercrime continues at an alarming rate and medical data continues to be one of the most valuable commodities for theft. We urge OCR to take these realities into consideration as it moves forward to modernize policies related to HIPAA and the breach of data in covered entity facilities.

If AHIMA can provide any further information, or if there are any questions regarding this letter and its recommendations, please feel free to contact Andrew Tomlinson, Director of Regulatory Affairs at andrew.tomlinson@ahima.org.

Sincerely,

Wylecia Wiggs Harris, PhD, CAE
Chief Executive Officer
AHIMA