



**Association of
American Medical Colleges**
655 K Street, N.W., Suite 100, Washington, D.C. 20001-2399
T 202 828 0400
www.aamc.org

Submitted via www.regulations.gov

June 6, 2022

Lisa J. Pino
Director
Office for Civil Rights
U.S. Department of Health and Human Services
Attention: HITECH Act Recognized Security Practices Request for Information
Hubert H. Humphrey Building, Room 509F
200 Independence Avenue SW
Washington, DC 20201

RE: Considerations for Implementing the Health Information Technology for Economic and Clinical Health (HITECH) Act, as Amended [RIN 0945-AA04]

Dear Director Pino:

The Association of American Medical Colleges (AAMC) appreciates the opportunity to respond to the Office for Civil Rights (OCR) Request for Information entitled “Considerations for Implementing the Health Information Technology for Economic and Clinical Health (HITECH) Act, as Amended,” 87 *Fed. Reg* 19833 (April 6, 2022).

The AAMC (Association of American Medical Colleges) is a nonprofit association dedicated to improving the health of people everywhere through medical education, health care, medical research, and community collaborations. Its members comprise all 155 accredited U.S. and 16 accredited Canadian medical schools; approximately 400 teaching hospitals and health systems, including Department of Veterans Affairs medical centers; and more than 70 academic societies. Through these institutions and organizations, the AAMC leads and serves America’s medical schools and teaching hospitals and the millions of individuals employed across academic medicine, including more than 191,000 full-time faculty members, 95,000 medical students, 149,000 resident physicians, and 60,000 graduate students and postdoctoral researchers in the biomedical sciences. In 2022, the Association of Academic Health Centers and the Association of Academic Health Centers International merged into the AAMC, broadening the AAMC’s U.S. membership and expanding its reach to international academic health centers. Learn more at aamc.org.

AAMC member hospitals and health systems have been leaders in ensuring that patient information is protected and are committed to using the best available security practices and standards. The HITECH Act was amended in 2021 to encourage Health Insurance Portability and Accountability Act of 1996 (HIPAA) covered entities and business associates to adopt strong cybersecurity practices by requiring OCR to consider such practices when imposing penalties or taking other enforcement actions. This is in part a recognition of the changing landscape from the law’s original passing in 2009, including ransomware and other cyber threats that may leave entities vulnerable even with the best security practices. In such an environment, it is critical to coordinate responses and share information to

strengthen defenses and avoid future harm. **The AAMC recommends OCR follow Congress’s lead and implement the amended HITECH Act provisions to encourage compliance, cooperation, and coordination in the face of common cyber threats and direct resources to supporting and advancing these goals.**

The HITECH Act, as originally passed by Congress, also requires OCR to establish a methodology for distributing a percentage of any civil monetary penalty or monetary settlement (collectively, “CMPs”) to harmed individuals, and OCR seeks feedback to inform these efforts. Under the Act, OCR has broad discretion to implement the statutory requirement. The AAMC recommends OCR develop an implementation methodology that reflects OCR’s primary focus as a regulatory agency, which is less suited to distributing compensation than a judicial body. OCR should not divert funding or resources from its regulatory role and responsibilities. **To this end, we believe OCR should limit award distributions to situations where there is a sufficiently large total settlement amount and clear economic harm and adopt a distribution methodology that is simple and efficient.**

We provide specific comments below on select questions.

RECOGNIZED SECURITY PRACTICES (PUBLIC LAW 116-321)

OCR Should Broadly Recognize Security Practices That Fall Within the Statutory Definition

OCR asks which recognized security practices regulated entities have implemented or plan to implement. Health care providers generally adopt risk-based security programs based on the factors listed in the HIPAA Security Rule,¹ which employs a flexible approach to allow entities to implement security practices most suited to their environment, operations, and risks. Some AAMC members obtain HITRUST certification, which provides a comprehensive and flexible framework drawing on National Institute of Standards and Technology (NIST), HIPAA, Payment Card Industry (PCI), and other security guidelines or standards. Many are increasingly adopting the Cybersecurity and Infrastructure Agency (CISA) cybersecurity recommendations and best practices. Regulated entities may also use a combination of different practices, standards, and guidelines for different parts of their business and operations.

The legislation defines security practices broadly to include not only standards, guidelines, processes, and procedures under the NIST Act or the Cybersecurity Act of 2015, but also any “programs and processes that address cybersecurity” as long as they are “developed, recognized, or promulgated through regulations under other statutory authorities.”² The legislation also makes clear that the specific practices adopted “shall be determined” by regulated entities, with the only condition being that the practices are consistent with the HIPAA Security Rule.³ **The Act defines the term in a carefully calibrated manner to remain broad while still providing sufficient clarity for regulated entities to understand the parameters of the term. We urge OCR to employ the statutory definition without further limitation.**

¹ See 45 CFR 164.306(b)

² See Sec. 13412(b)(1) of P.L. 116-321

³ Ibid.

OCR Should Apply a Standard Based on Compliance Best Practices for Assessing Whether a Covered Entity Had Recognized Security Practice in Place 12 Months Prior to a Violation

OCR asks what standards it should implement to assess whether a recognized security practice was “in place” 12 months prior to a potential HIPAA violation. Consistent with the requirements of the HIPAA Security Rule, regulated entities perform periodic risk analyses and updates to their risk management plans. This includes confirming that the security practices adopted by the entity have been properly implemented and are operating as intended. Compliance program best practices are built around plans designed to identify risks, document risks, evaluate risks, and audit. Simply put, in large and complex organizations it is unlikely that any compliance system can constantly monitor, assess, and demonstrate that a practice is in place at each and every system entry point or terminal. Setting an unreasonable standard for assessing whether the security practice was active and consistent across the enterprise for 12 months would frustrate the intent of the statute, which is to incent broader adoption of stronger security safeguards. **The AAMC recommends that OCR take into consideration all recognized security practices to the extent that they have been implemented, rather than adopt an all-or-nothing view of “in place.” Additionally, the AAMC urges OCR to limit the standard to one that is clear and that can be readily assessed, rather than one that is subjective.**

ESTABLISHING A METHODOLOGY TO DISTRIBUTE A PORTION OF MONETARY SETTLEMENTS OF PENALTIES TO INDIVIDUALS HARMED BY VIOLATIONS OF THE HIPAA RULES (SECTION 13410(C)(3) OF THE HITECH ACT

OCR Should Limit Compensable Harm to Instances of Clearcut Economic Harm

While there is no question that individuals may suffer both economic and noneconomic harms from HIPAA violations, this does not mean that all such harms should be compensable through the mechanism contemplated in Section 13410(c)(3) of the HITECH Act. Instead, consideration should be given to the suitability of the mechanism in question for determining certain types of harm, and the potential for inconsistent and potentially inequitable outcomes resulting from use of a mechanism not designed for making such calibrations. Given the difficulty and subjectivity involved in determining noneconomic harm, both as to type and appropriate compensation, and the fact that a regulatory agency such as OCR is ill-suited to gathering the facts and evidence necessary to make such determinations accurately or equitably, we recommend that OCR limit its consideration to economic harms.

OCR Should Limit Its Recognition of Compensable Harm to Only Those Individuals Whose PHI was Impermissibly Released

OCR asks whether it should recognize as harm the release about a person other than the individual who is 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. We recommend that OCR prioritize consistency with its own guidance distinguishing that another person’s information included in a patient’s individual record is the patient’s PHI (and not the other person’s)⁴ We

⁴ See HHS OCR Guidance [The HIPAA Privacy Rule: Frequently Asked Questions About Family Medical History Information](#) (stating “When a covered health care provider, in the course of treating an individual, collects or otherwise obtains an individual’s family medical history, this information becomes part of the individual’s medical record and is treated as “protected health information” about the individual. Thus, the individual (and not the family members included in the medical history) may exercise the rights under the HIPAA Privacy Rule to this information

believe consistency of application of the definition of an individual's PHI provides necessary clarity for regulated entities. OCR should limit the recognition of compensable harm only to those individuals whose PHI was impermissibly released, and that in the case of family history, the individual alone should be eligible for compensation for economic harm resulting from an impermissible release.

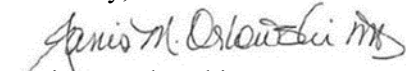
OCR Should Apply a Case-by-Case Determination of the Total Amount for Compensable Harm Distribution

OCR asks several questions regarding whether there should be a minimum total settlement or penalty amount before setting aside funds for distribution and whether there should be a minimum amount available per harmed individual. Consistent with the approach adopted by other agencies mentioned in the RFI, such as the Consumer Financial Protection Bureau ("CFPB") and the Security Exchange Commission ("SEC"), **OCR should have the discretion, on a case-by-case basis, to determine whether the total settlement or penalty amount is sufficient for distribution.** This will allow OCR to account for the many varied factors that could affect the practicability of making a distribution in a particular case, including, but not limited to, the difficulty in determining harm, locating those harmed, measuring harm, determining the number of individuals affected, and when the impermissible use or disclosure resulting in harm occurred.

CONCLUSION

Thank you for this opportunity to provide comments to inform the development of future guidance or rulemaking to inform providers on the application of the new law regarding security practices and policies for a future compensation distribution methodology. We remain committed to work with OCR on any of the issues discussed above or related topics that impact the teaching hospital and academic health center community. If you have questions regarding our comments, please feel free to contact Phoebe Ramsey, pramsey@aamc.org.

Sincerely,



Janis M. Orlowski, M.D., M.A.C.P.

Chief Health Care Officer

cc: David J. Skorton, M.D., President and CEO, AAMC
Phoebe Ramsey, J.D., AAMC
Ivy Baer, J.D., AAMC

in the same fashion as any other information in the medical record, including the right of access, amendment, and the ability to authorize disclosure to others.”)