EHRA
HIMSS ELECTRONIC HEALTH RECORD ASSOCIATION

350 North Orleans Street, Suite S10000
Chicago, IL 60654

@EHRAssociation | ehra.org

June 6, 2022

Lisa J. Pino
Director, Office for Civil Rights
U.S. Department of Health & Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

Dear Ms. Pino,

On behalf of our 30 member companies, the HIMSS Electronic Health Record Association (EHRA) is pleased to provide feedback on Considerations for Implementing the Health Information Technology for Economic and Clinical Health (HITECH) Act, as Amended. We appreciate the opportunity to provide comments on the consideration of recognized security practices of covered entities and business associates.

As a national trade association of electronic health record (EHR) developers, EHRA member companies serve the vast majority of hospital, post-acute, specialty-specific, and ambulatory healthcare providers using EHRs and other health IT across the United States, including by supporting the numerous practices they have adopted to secure sensitive patient information. Together, we work to improve the quality and efficiency of care through the adoption and use of innovative, interoperable, and secure health information technology.

Although HIPAA breaches in the past have been caused by regulated entities' mishandling of protected health information, today, they are often a result of cyberattacks, ransomware, or other malicious activity leveled against healthcare organizations. Because of this shift in the risks faced by regulated entities, we support OCR's efforts to implement provisions of the HITECH Act that recognize entities' efforts to secure protected health information. Given that implementing recognized security practices doesn't mean an organization is hack-proof, victims of cyberattacks that have operated in good faith to secure health information should not be penalized as if they willfully committed the breach if they have implemented cybersecurity best practices. It is important to cultivate a culture in which organizations do not feel that they will be blamed unreasonably, as the victims of cyberattacks, but rather are recognized for adopting available technologies and training staff wherever possible.

Further, OCR notes that the statute does not require rulemaking, and that any comments will inform future guidance or rulemaking. EHRA strongly encourages OCR to consider rulemaking to implement

AdvancedMD
Allscripts
Athenahealth
BestNotes
Cerner Corporation
CPSI
CureMD
eClinicalWorks
eMDs
Endosoft
Epic
Experity
Flatiron Health
Foothold Technology
Greenway Health
Harris Healthcare Group
Lumeris
MatrixCare
MEDHOST
MEDITECH, Inc.
Medsphere
Modernizing Medicine
Netsmart
Nextech
NextGen Healthcare
Office Practicum
Sevocity
STI Computer Services
TenEleven Group
Varian

Public Law 116-321. This will allow stakeholders an opportunity to comment on the specific approach proposed by OCR, as opposed to providing only more general information on current security practices to help inform OCR in developing its approach. This is especially important to ensure that the manner in which OCR implements the statute achieves its goal of encouraging regulated entities to do “everything in their power to safeguard patient data” while maintaining flexibility for regulated entities to implement and improve their cybersecurity practices in response to each entity’s evolving risk assessments. This will be possible only if regulated entities understand how OCR will implement the statute, can maintain flexibility to modify and enhance their cybersecurity practices as the threat landscape evolves, and also believe that their efforts to implement security practices will make a material difference to the enforcement action they could potentially face. It is only through notice and comment rulemaking that OCR can obtain this essential feedback and provide the assurance of a flexible, consistent, and practical approach.

We offer the following considerations regarding the Request for Information.

Sincerely,

Hans J. Buitendijk
Chair, EHR Association
Cerner Corporation

David J. Bucciferro
Vice Chair, EHR Association
Foothold Technology

HIMSS EHR Association Executive Committee

Pamela Chapman
Experity

William J. Hayes, M.D., M.B.A.
CPSI

Barbara Hobbs

Barbara Hobbs
MEDITECH, Inc.

Cherie Holmes-Henry
NextGen Healthcare

Stephanie Jamison
Greenway Health

Alya Sulaiman, JD
Epic

Established in 2004, the Electronic Health Record (EHR) Association is comprised of nearly 30 companies that supply the vast majority of EHRs to physicians’ practices and hospitals across the United States. The EHR Association operates on the premise that the rapid, widespread adoption of EHRs will help improve the quality of patient care as well as the productivity and sustainability of the healthcare system as a key enabler of healthcare transformation. The EHR Association and its members are committed to supporting safe healthcare delivery, fostering continued innovation, and operating with high integrity in the market for our users and their patients and families. The EHR Association is a partner of HIMSS. For more information, visit www.ehra.org.

Regulated entities' implementation of "recognized security practices"

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

EHRA Response:
Examples of industry-recognized frameworks commonly utilized by stakeholders include the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), the International Organization for Standardization and the International Electrotechnical Commission ISO/IEC 27001, Statement on Standards for Attestation Engagements (SSAE) (SSAE 18 SOC2), and the HITRUST Cybersecurity Framework. Many cybersecurity best practices, however, are shared across cybersecurity frameworks or could be implemented independently of whether an organization adheres to a specific framework.

The EHRA encourages OCR to promote innovation and broad adoption of cybersecurity best practices by recognizing the inherent value of the implementation of *any* recognized security practices, rather than attempting to prescribe one narrowly designed set of security practices. Security frameworks address different types of risks and as technology or best practices evolve, their utility to any certain regulated actor may also change. If a regulated entity adopts a practice with the purpose of mitigating a risk it faces, OCR should recognize the practice.

What other programs and processes that address cybersecurity and that are developed, recognized, or promulgated through regulations under other statutory authorities do regulated entities rely on when establishing and implementing recognized security practices?

EHRA Response:
Health IT certification requirements from the Office of the National Coordinator for Health Information Technology (ONC) include criteria for security, including requirements to support audit logging and tamper-resistance features that healthcare organizations might use as part of their efforts to ensure the security of protected health information. Additionally, healthcare organizations that electronically prescribe controlled substances are subject to security requirements from the Drug Enforcement Administration (DEA). Many also adhere to cybersecurity programs/frameworks used in the financial services sector, such as PCI Security Standards, in order to process payments from patients.

What steps do covered entities take to ensure that recognized security practices are "in place"?

EHRA Response:
First, it is important to recognize that a security breach or incident doesn't necessarily mean the organization is non-compliant with the HIPAA security rule. For example, an overworked nurse in a COVID-19 unit may accidentally click on a phishing email, but this momentary lapse of judgment is not an indication that the hospital is broadly non-compliant.

Covered entities and business associates verify security practices through such approaches as internal and external audits, risk assessments, threat risk assessments, and privacy impact assessments. Specific criteria for many audit frameworks are defined by the implemented cybersecurity framework, such as NIST, HITRUST, or using OCR's HIPAA assessment tool, for example. Audit frameworks, like SOC 2 Type 2 audits, provide a standard methodology to validate that the practices are in place as described. In general, organizations showing that they have a process for validating that security practices are in place should be recognized as having implemented cybersecurity practices.

Given the varied applicability of specific security practices throughout the organization of a covered entity, EHRA encourages OCR to place emphasis on meeting the scope of applicability of a given practice rather than seek to narrowly define whether a practice was in place for a set of physical or technical infrastructure.

What steps do covered entities take to ensure that recognized security practices are actively and consistently in use continuously over a 12-month period?

EHRA Response:
It is important for organizations to be encouraged to update security practices regularly as new technologies or methodologies evolve. We are concerned that a strict interpretation of security practices "actively and consistently in use continuously" over a 12-month period could have the unintended consequence of discouraging the adoption of new methods during that time frame. Organizations should retain the flexibility to update processes throughout the year to meet ever-changing cybersecurity best practices without concern of running afoul of the requirement for consistent and continuous use. **EHRA again recommends OCR distinguish between confirming that a control is in place and narrowly defining how the control is implemented.**

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.

EHRA Response:
HIPAA breaches often impact many thousands of people at a time. This scale of compensable damage makes delivering meaningful compensation to affected individuals challenging. **EHRA suggests that a more impactful use of collected fines and OCR's resources would be in the creation and distribution of educational materials and additional resources for covered entities.** Doing so will support improved compliance and continuous updating of best practices for maintaining cybersecurity programs.