June 6, 2022

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

Submitted electronically via www.regulations.gov

Dear Director Pino:

On behalf of the Healthcare Information and Management Systems Society (HIMSS), I am pleased to provide written comments in response to the Request for Information on Considerations for Implementing the Health Information Technology for Economic and Clinical Health (HITECH) Act, as Amended. HIMSS applauds the work of the Office for Civil Rights (OCR) in looking for how covered entities and business associates are voluntarily implementing recognized security practices as identified in Public Law 116-321, the recent HITECH Security Practices Amendments, and public input on potential information or clarifications OCR could provide on its implementation of the statute in future guidance or rulemaking.

HIMSS is a global advisor and thought leader supporting the reform of the global health ecosystem through the power of information and technology. As a mission-driven non-profit, HIMSS offers a unique depth and breadth of expertise in health innovation, public policy, workforce development, research, and analytics to advise global leaders, stakeholders, and influencers on best practices in health information and technology. Through our innovation engine, HIMSS delivers key insights, education, and engaging events to healthcare providers, governments, and market suppliers, ensuring they have the right information at the point of decision. Established in 1961, HIMSS serves the global health information and technology communities with focused operations across North America, Europe, the United Kingdom, the Middle East, and Asia Pacific. Our members include more than 130,000 individuals, 480 provider organizations, 470 non-profit partners, and 650 health services organizations across 86 countries.

Applicability of the New Law

In our recently updated Public Policy Principles, HIMSS notes the importance of a unified approach to healthy cybersecurity and information privacy practices emphasized in the HITECH Security Practices Amendments in Public Law 116-321. Under the law, the U.S. Department of Health & Human Services (HHS) is given the specific authority to consider whether a covered entity or business associate, as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), has adequately demonstrated that it had, not less than the previous 12 months, recognized security practices in place. If such recognized security practices have been adequately demonstrated, these may help mitigate potential fines, result in early, favorable determination of an audit, and initiate the remedies that might otherwise be agreed to in resolving potential HIPAA Security Rule violations. We recommend OCR implement policies that only afford enforcement discretion to situations involving use of security best practices as that discretion applies to safeguarding electronic protected health information (PHI) and not to other areas that are within the scope of HIPAA.

Recognized Security Practices Implemented by Regulated Entities

HIMSS encourages OCR to foster innovation in standards by recognizing the inherent value of adherence to widely accepted cybersecurity frameworks and standards that have been adopted by industry, rather than attempting to prescribe a fixed set of cybersecurity practices that risk becoming stagnant in an ever-evolving threat environment. For example, HIMSS strongly encourages our members to use and provide feedback to the NIST Cybersecurity Framework (CSF), which is regularly updated with stakeholder input, and discussed more below.

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

Healthcare security has grown dramatically over the past seven years. For healthcare, coordination and sharing best practices have accelerated as a result of the healthcare-specific provisions in the Cybersecurity Act of 2015.,

As a driving force behind the legislations that created Section 405(d) in the Cybersecurity Act of 2015, HIMSS is encouraged to see what we know to be a growing use of the 405(d)'s Health Industry Cybersecurity Practices (HICP), which were first released January 2, 2019, following more than one year of pre-testing. The HCIP was developed under one of the standing task groups of the HSCC Cybersecurity Working Group, of which HIMSS is an active member.

As part of these efforts, HIMSS strongly supports using the NIST CSF. As we have seen over the past several years, stakeholders across several regulated industries, including critical infrastructure sectors such as healthcare, financial, energy, telecommunications, and information technology, have adopted the CSF. The CSF is highly useful to healthcare organizations of all types and sizes.

The CSF is widely used by many healthcare organizations to manage cybersecurity risk more effectively. The five functions of Identify, Detect, Protect, Respond, and Recover provide a practical outline for organizations to navigate data protection in cyberspace. The cycle of continuous improvement built into the CSF process increases the likelihood the resources are current and healthcare organizations have more secure practices in place.

Additionally, many healthcare organizations have adopted the sector specific HITRUST Common Security Framework, which has also been mapped to CSF. In terms of standards and best practices, the ISO/IEC 27000 series, and NIST Special Publication No. 800-53 Revision 5 are widely used by healthcare stakeholders.

Finally, HIMSS takes a lot of pride in the nearly 30-year commitment to educating the healthcare community on preparation and mitigation of privacy, security, and cybersecurity threats. Built on the foundation of our industry-leading security toolkit that was first established in the 1990s, the HIMSS Cybersecurity Guide provides a practical starting point on current threats, best practices, and other important preparedness topics. The Cybersecurity Guide is continually informed by our HIMSS Cybersecurity Report, an annual survey of industry leaders and frontline cybersecurity professionals.

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?

HIMSS recommends OCR align its work with other federal agencies to improve best practices for healthcare. Among the many examples of regulatory and statutory requirements HIMSS members track, we find our members are subject to the security requirements for controlled substances from the Drug Enforcement Administration (DEA), cybersecurity programs/frameworks used in the financial services sector to process payments from patients, as well as the Health IT certification requirements from the Office of the National Coordinator for Health Information Technology (ONC) including criteria for security, audit logging, tamper-resistance, and similar functionality.

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

As referenced earlier in our letter, the HIMSS Cybersecurity Guide provides threats and response best practices for organizations and employees to incorporate into their daily security practices. By and large, covered entities and business associates regularly perform risk assessments and privacy impact assessments. Covered entities and business associates also utilize internal audits and third-party audits for compliance purposes. Policies and procedures are periodically developed, vetted, and revised in alignment with then current practices. Security awareness training, at minimum, includes training on phishing and compliance with HIPAA requirements.

Additionally, many stakeholders encourage employees, staff, and others to report suspected or known incidents as soon as possible to the appropriate point(s) of contact. Further, many stakeholders also have programs in place to help detect and mitigate insider threat from employees, contractors, and others with trusted access to systems and networks. Finally, yet importantly, supply chain considerations should also be considered, including selection, vetting, and management of third-party suppliers and vendors.

Nonetheless, cybersecurity is indeed a moving target. The most secure systems of today might not necessarily be secure tomorrow. The physical, technical, and administrative safeguards that are in place can have a wide variation—but one size does not fit all. Rather, it is the alignment of people, processes, and technology with administrative, physical, and technical safeguards that can help fortify any organization's cybersecurity program. But it should be emphasized, too, that compliance does not equal security. Additionally, the state of the art today will have limitations tomorrow, some of which we can foresee and others which we cannot, especially when considering the actions of sophisticated nation states or non-state actors. That is why industry best practices must remain fluid and cannot necessarily be prescribed by way of regulation (or statute). Considering this, healthcare stakeholders and others are engaged in appropriate information sharing regarding threats, actual incidents, and mitigations—within their own organizations, with other peers in industry, and yet others across other critical infrastructure sectors.

Many healthcare stakeholders, too, are aware of the global nature of healthcare cybersecurity—especially since these stakeholders often exchange electronic health information across national and regional borders and because the supply chain is, indeed, global. Some stakeholders have multiple sites around the world, many stakeholders rely on third party services for creating, receiving, transmitting, or maintaining electronic protected health information. Some of these third-party services are located outside of the United States, and virtually all stakeholders use devices and equipment that are sourced from or that otherwise have components from outside of the United States. This, too, is a concern, given the lack of explicit extraterritorial reach of HIPAA (unlike the EU GDPR, for instance).

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

It is important for organizations to be encouraged to update security practices regularly as new technologies or methodologies emerge. We are concerned that a strict interpretation of security practices in place 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. HIMSS recommends OCR distinguish between confirming that a control is in place and narrowly defining how the control is implemented.

Additional information to consider in developing guidance or a proposed regulation regarding the consideration of recognized security practices.

While not every breach is the result of a HIPAA violation, patient safety is at risk whenever there is a compromise of protected health information. However, in the case of actual HIPAA violations, compensation to affected individuals may not necessarily make them whole, especially when the impact is non-pecuniary in nature (e.g., patient harm or medical identity theft and fraud concerns).

Cybersecurity is a success when organizations work together to spread the news on alerts, preparedness best practices, and mitigation strategies. HIMSS recommends OCR embrace the culture of learning to ensure all organizations have the knowledge and resources to prevent or mitigate attacks from bad actors. HIMSS 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, business associates, and others (such as, but not limited to, organized health care arrangements, subcontractors, market suppliers, and others). Doing so is more likely to support improved compliance and continuous updating of best practices for maintaining cybersecurity programs.

HIMSS welcomes the opportunity to be a resource to OCR on innovative, forward-thinking steps to educate the public around cybersecurity practices and data privacy. We look forward to the opportunity to discuss these issues in more depth. Please feel free to contact Eli Fleet, Director of Government Relations Eli.Fleet@himss.org with questions or for more information.

Thank you for your consideration.

Sincerely,

Thomas M. Leary

Thomas M. Leary, MA, CAE, FHIMSS
Senior Vice President and Head of Government Relations
HIMSS