

November 30, 2022

The Honorable Mark Warner
US Senate
703 Hart Senate Office Building
Washington, DC 20510

RE: Response to “Cybersecurity is Patient Safety: Policy Options in the Health Care Sector”

Submitted via email to cyber@warner.senate.gov

Dear Senator Warner:

Thank you for the opportunity to provide feedback on the state of cybersecurity within the US healthcare system. As our healthcare system becomes increasingly interoperable and electronic, we must ensure that we proactively address cybersecurity threats that may compromise both patient safety and privacy. We applaud your continued leadership in this area.

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. AHIMA’s 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. AHIMA members also bring the expertise and knowledge around health information and data that is necessary to inform investments in our healthcare system, including cybersecurity.

We appreciate the commitment to addressing challenges associated with cybersecurity in our healthcare system. AHIMA offers the following feedback in response to questions posed by the Request for Information.

1.1 – Healthcare Cybersecurity Leadership within the Federal Government

A robust cybersecurity framework within the healthcare system requires clear and comprehensive leadership, guidance, and enforcement from the federal government. In doing so, policy must also work to ensure health organizations are not beholden to inconsistent, duplicative or conflicting data protection standards of compliance between state and federal regulations. Policy must work to ensure that legislation and regulations seeking to address information security, cybersecurity, and privacy are complementary, including the harmonization of definitions across all areas.

The Health Insurance Portability and Accountability Act (HIPAA) and its subsequent Privacy and Security Rules provide protection for covered healthcare information. However, as technology has advanced, new tools and solutions for storing and exchanging health information have come to market and are not necessarily covered under the HIPAA framework. AHIMA encourages Congress to ensure comprehensive privacy legislation is considered along any cybersecurity policies, such as H.R. 8142, the “American Data Privacy and Protection Act.”

In the HHS efforts around improving cybersecurity, including the efforts to reexamine the HHS Breach Portal, maintaining consumer notifications of breaches is vital. These efforts will be strengthened by differentiating between health organizations that are the victim of a breach but work in good faith to protect patient data by implementing industry standard cybersecurity best practices, and those organizations who do not work in good faith to protect against a breach. With the HHS Breach Portal, HHS should develop processes for health organizations to remove their name from the list demonstrating that security issues have been resolved and appropriate tools and protocols have been implemented. It is also important to encourage the Office for Civil Rights (OCR) to continue to move on rulemaking associated with “recognized cybersecurity best practices” as a mitigating factor when determining fines, audits, and remedies against covered entities.

1.6 – Workforce Development Program that Focuses on Healthcare Cybersecurity

AHIMA agrees that a workforce development program focusing on healthcare cybersecurity should be a priority in any policy addressing cyber threats in the US. Policy may include new training programs specific to training those new to healthcare cybersecurity, but AHIMA believes it should also include federal funding or incentives for training or certifications specific to professionals already in areas such as healthcare information security, cybersecurity, privacy, and health information management, to encourage advanced cybersecurity skills and upskill the current workforce. We must ensure that cybersecurity is a priority among many departments within health organizations, and that all employees who handle patient information have the processes, skills, and technology needed to ensure the security of all patient health information, including times in which health IT systems may go offline amid a cybersecurity incident.

2.4 – Streamlining Information Sharing

The need to streamline information sharing around cyberattacks is clear. AHIMA sees the need to enhance and improve information sharing of cyber threats, risks, and cyber hygiene practices in real time. To do that, any policy must prioritize engagement of all healthcare industry stakeholders and align with cross-sector cyber threat information sharing activities, ensuring information is tailored toward multiple levels of organizational size, capacity, and venue, and implemented consistently while preserving patient confidentiality and privacy. Congress should also ensure all federal entities responsible for cyberthreat notification collaborate to ensure messaging is consistent across the whole of government.

It is also clear that any information sharing and reporting must be bidirectional and collaborative – information reported to the government needs to be promptly aggregated, anonymized, analyzed, and shared to foster future cyber incident mitigation and prevention strategies.

AHIMA thanks Senator Warner for his leadership in strengthening our healthcare system and for the opportunity to provide feedback. We look forward to working with you to ensure a healthcare system that is prepared to handle the cyberattacks we are seeing today. Should you or your staff have any additional questions or comments, please contact Kate McFadyen, Director, Government Affairs, at kate.mcfadyen@ahima.org or (202) 480-6058.

Sincerely,

A handwritten signature in black ink, appearing to read "Lauren Riplinger", is centered on a light gray rectangular background.

Lauren Riplinger
Vice President, Policy & Government Affairs