AHIMA Policy Statement on Cybersecurity and Information Security[1]

AHIMA's Position:

AHIMA supports the use of policy to address the information security, including cybersecurity, of patients' health information. Health information (HI) professionals have extensive knowledge and expertise to contribute in developing these policies. It is vital that any legislation or regulation that addresses cybersecurity or information security must consider the people, processes, and technologies that affect cybersecurity. To make the strides needed in cybersecurity within healthcare, AHIMA believes that policy must:

1. **Enhance and improve information sharing of cyber threats, risks, and cyber hygiene practices in real time.** 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.

2. **Support each principle of the CIA triad[2] (confidentiality, integrity, availability) at the highest level possible.** Policy must support organizations' ability to keep data confidential, ensure the integrity of the data, and ensure authorized users have timely, reliable access to data.

3. **Provide strong and clear leadership from the federal government.** Policy must ensure that there is clear and comprehensive leadership, guidance, and enforcement from the federal government.

4. **Harmonize laws and regulations, including state and federal laws.** Policy must work to ensure that health organizations are not beholden to inconsistent and conflicting data protection standards of compliance. Policy must also 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.

5. **Provide funding and/or incentives to bolster the healthcare workforce and resources for information security and cybersecurity.** Policy should include federal funding or incentives for training or certifications specific to healthcare information security, cybersecurity, privacy, and HI professionals to encourage advanced cybersecurity skills. Policy should also foster incentives to encourage a workforce that has expertise across all of these areas.

---

[1] Information security encompasses confidentiality, integrity, and availability of health data, and cybersecurity specifically protects electronic data.

[2] The CIA Triad is a well-known, venerable model for the development of security policies used in identifying problem areas, along with necessary solutions in the arena of information security. https://www.forcepoint.com/cyber-edu/cia-triad

Background:

Data breaches are an ever-growing threat in healthcare. The average total cost of a data breach in the healthcare industry is $6.45 million: 65 percent higher than the average data breach across all sectors.[3] While the monetary costs of a data breach are unsustainable, the more immediate danger is to patients. Data breaches put patients at risk of identity theft, fraud, and compromised medical data.

While steps have been taken to increase cybersecurity in the healthcare field, there is still a patchwork of laws and regulations and a lack of resources that must be improved and harmonized. As policymakers seek to address this issue, AHIMA members have the expertise to offer practical insight.

Key Points:

Improved cybersecurity measures could result in considerable benefits, including:

- Reduced risk of patient identity theft, fraud and compromised medical data;
- Improved patient information security;
- Reduced liability for healthcare organizations;
- Enhanced relationships and data sharing between security and privacy professionals;
- Increased public trust in healthcare institutions and their security measures; and
- Less wasted resources used in addressing data breaches.

To realize the benefits of improved cybersecurity for the healthcare industry, certain barriers must be addressed, including:

- **Challenges to information sharing** including technological barriers, such as a lack of interoperability or hardware/software capabilities; informational barriers, such as unreliable data; and organizational barriers, including lack of resources and organizational policies.[4]
- **Lack of harmonization of laws and regulations.** The US regulates certain sectors and types of information differently, creating overlapping and sometimes contradictory protections. State laws and regulations can also add an additional layer of complexity with varying definitions, measures, and regulations that are often incompatible.[5]
- **Insufficient personnel and funding.** According to a study conducted by the Ponemon Institute, only 30 percent of respondents rate their organization's IT security effectiveness at mitigating risks, vulnerabilities, and attacks as "very high." The most

[3] IBM Security: Cost of a Data Breach Report 2019. Available at: https://databreachcalculator.mybluemix.net/complete-findings
[4] https://cams.mit.edu/wp-content/uploads/2017-13.pdf
[5] Reforming the U.S. Approach to Data Protection and Privacy. Available at: https://www.cfr.org/report/reforming-us-approach-data-protection

cited challenges in achieving this level of effectiveness are insufficient personnel and insufficient budget.[6] There is also a lack of personnel with expertise across both privacy and security.

- **Need for additional federal support.** Cybersecurity must be a top priority for the federal government across all sectors, especially the healthcare sector. Federal support must be adequate to facilitate information sharing, the creation of best practices, and the monitoring of cyber threats.

Current Situation:

The Cybersecurity Act of 2015 created a framework for sharing cyber threat information among the federal government and the private sector. Title I, the Cybersecurity Information Sharing Act of 2015 (CISA), attempted to mitigate the private sector's reluctance to share information that could expose them to civil or criminal liability. CISA authorized private companies to share cybersecurity threat information for "cybersecurity purposes" with the federal government and other private entities. The Cybersecurity Act also required the HHS to report on how the healthcare industry prepares for cyberattacks and threats.

In June 2017, that report was finalized and presented to Congress. The "Report on Improving Health Care Industry Cybersecurity" was created by the Health Care Industry Cybersecurity Task Force, a public-private task force that sought input from government, industry, outside stakeholders, and the general public. The report resulted in the development of six imperatives that resulted in a number of recommendations and action items. While many of these recommendations have been put into action, there are still improvements that need to be made and actions that need to be taken, including the policy recommendations AHIMA has put forth here.

In 2018, HHS created the Health Sector Cybersecurity Coordination Center to strengthen information sharing with the healthcare and public health sectors and provide intelligence to health organizations. Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients is the primary publication of the Cybersecurity Act of 2015, which aims to raise awareness, provide vetted cybersecurity practices, and move organizations towards consistency in mitigating the current most pertinent cybersecurity threats to the sector.

Despite these developments, cyberattacks continue to be a problem. Keeper Security's *2019 Global State of Cybersecurity in Small and Medium-Sized Businesses* report found that nearly two-thirds of healthcare organizations globally have experienced a cyberattack in their lifetime, and over half were attacked within the last year.[7] Data breaches in healthcare resulted in an average of 7,202 patient and employee records lost or stolen, and yet less than half of those surveyed have a plan for responding to a cyberattack.[8]

A number of bills in the 116th Congress address a range of cybersecurity measures, including legislation that would provide grants for secondary and post-secondary cybersecurity education,

[6] 2019 Global State of Cybersecurity in Small and Medium-Sized Businesses. Available at: https://www.keeper.io/hubfs/2019%20Keeper%20Report_Final%20(1).pdf
[7] https://start.keeper.io/2019-ponemon-report
[8] https://www.securitymagazine.com/articles/91880-of-healthcare-organizations-globally-have-experienced-cyberattacks

increase security around the Internet of Things (IoT), establish a Cybersecurity State Coordinator in each state, and promote patient data security.

AHIMA stands ready to contribute to the conversation around cybersecurity in the healthcare sector.