Cybersecurity and Data Privacy

Ensuring the privacy and security of patient health information.

Cybersecurity in healthcare involves the protecting of *electronic* information and assets from unauthorized access, use and disclosure. There are three goals of cybersecurity: protecting the *confidentiality*, *integrity* and *availability* of information, also known as the "CIA triad."

Healthcare has been identified as the number one target of cybercriminals. An information sharing pipeline that allows the government to inform the private sector of cyber threat intelligence should be created.

The 2020 HIMSS Cybersecurity Survey notes that Phishing remains a significant threat. **Most significant security incidents are a result of successful phishing attempts.**

Physical security is also a factor in protecting data. Unauthorized physical access to a computer or device may lead to its compromise. Physically securing a device is important to safeguard its operation, proper configuration and data.

Health Sector Coordinating Council's Cybersecurity Work Group, the National Healthcare Information Security Advisory Council, and the Health Sector Cybersecurity Coordination Center, these entities should receive expanded resources to combat the increasing cybersecurity challenges facing healthcare.

U.S. Health Data Privacy Compliance Challenges

- As new market entrants enter healthcare, how we think about data privacy broadly also needs to evolve. HIMSS stresses that how HIPAA applies and intersects with other privacy regulations may be an unintended barrier for broader information sharing as well as efforts to better engage patients in their own care.
- HIMSS supports the development of a comprehensive health privacy law that encompasses all these issues from a broader perspective and one that is implementable.

Global Cybersecurity-Related Priorities

- On a global scale, HIMSS has been working with the International Red Cross and Peace Institute to support of broader cybersecurity protections for healthcare facilities across the globe.
- HIMSS is imploring governments to develop and embrace a Geneva Convention-like policy for the medical cyber space that is similar to the protections physical facilities receive near combat zones. We collaborated to call on the United Nations and governments worldwide to extend the protections for healthcare that occur around physical battlefields to cybersecurity, particularly to protect healthcare facilities from attacks by state-sponsored hackers.

Wins

- Section 405 C and D of Cybersecurity Act of 2015 [dedicated to healthcare cybersecurity] originated from HIMSS Congressional cybersecurity ask.
- H.R. 7898 (116th Congress), Public Law No: 116-321, amends the Health Information Technology for Economic and Clinical Health Act to allow HHS to reduce fines and penalties for violations of certain federal privacy standards for health information if an entity subject to those standards has adopted particular cybersecurity practices. This bill was brought on by efforts of HIMSS and the Healthcare Sector Coordinating Council Cyber Work Group.

Engagements

- Annual 2020 HIMSS Cybersecurity Survey which provides insight into the landscape of U.S. healthcare organizations based on feedback from 168 U.S.-based industry professionals.
- HIMSS staff was appointed as Team Leader of the Protecting Sensitive Information and Intellectual Property Team for the 2021 US DHS Analytic Exchange program.
- Healthcare Sector Coordinating Council Cyber Work Group.
- HIMSS Chapters, with guidance from HIMSS, successfully advocated for legislation advancing cybersecurity and data privacy at the state and local levels.