Cyber Threat Information-Sharing

September 2016

A recent news report indicated that criminal cyberattacks against health care entities have increased up to 125 percent compared to five years ago, and the average consolidated total cost of data breach was $3.8 million, which is a 23 percent increase from 2013 to 2015. One of the best tools to combat cyber threats is timely information. As such, Covered Entities and Business Associates should consider building information-sharing relationships within the health care industry.

Even the Federal Government has recognized the importance of information-sharing in the cybersecurity context. In 2015, Congress passed the Cybersecurity Information Security Act (CISA) and President Obama issued Executive Order 13691.

CISA encourages Covered Entities and Business Associates to help each other prepare for possible threats or vulnerabilities to ePHI systems by sharing information such as a description of the technical, physical, or administrative specifications related to threats to systems or vulnerabilities to systems, in addition a broad description of the harm caused by exploitation of these specifications.

Executive Order 13691 promotes healthcare sector cybersecurity information-sharing and encourages the development of Information Sharing and Analysis Organizations (ISAOs), that would serve as central points for cybersecurity relationships within the private sector and amongst the Federal Government and private sector. The ISAOs will share cyber threat information bi-directionally between HHS and the Health Care and Public Health (HPH) sector regarding cyber threats and will also provide outreach and education to the HPH sector. For

further information about joining the ISAOs membership, contact the ISAO Standards Organization at isao@lmi.org or DHS at isao@hq.dhs.gov.

Additionally, information-sharing involves communication and collaboration between different Covered Entities and Business Associates, which allows these organizations to work together and form trusted working relationships.

NIST's ***Guide to Cyber Threat Information Sharing*** identifies benefits and challenges for organizations participating in information sharing activities; benefits of information sharing include:

- Shared Situational Awareness – Enables organizations to leverage the collective knowledge, experiences, and analytic of their sharing partners, thereby enhancing the defensive capabilities of both organizations.

- Heightened Understanding of Cyber Threats – Allows entities to develop and share threat intelligence, which helps them, improve their understanding of the cyber threat environment and provide them the capability to tailor and deploy security controls, countermeasures, detection methods, and corrective actions based on detected changes in the threat environment.

- Improved Decision Making – Information-sharing enables organizations to make decisions with promptness and self-assurance.

Even though there are benefits to information-sharing, Covered Entities and Business Associates should consider the challenges as well, such as:

- Protecting Privacy – Although organizations may be able to participate in information-sharing program, some are still required to anonymize their contributions.

- Legal and Organization Restrictions – An organization's executive and legal teams may restrict the types of information that the organization can share. Restrictions may include limits on the types of information and the level of technical detail provided.

- Risk of Disclosing Sensitive Information - Disclosing sensitive information, such as PII, PHI, intellectual property, trade secrets, or other proprietary information can result in financial loss, violations of sharing agreements or federal regulations, legal action, and loss of reputation.

Furthermore, in order for Covered Entities and Business Associates to have a successful information-sharing program, entities should also factor in what key elements are needed to build, sustain, and utilize a trusting and transparent information-sharing relationship amongst each other.

For more information on what type of information can be disclosed by Covered Entities and Business Associates in this context, access the **Office for Civil Rights Cybersecurity Act 2015 (CISA) FAQ** *(Soon to be released)*.

Resources:

National Institute of Standardization and Technology (NIST) http://csrc.nist.gov/publications/PubsSPs.html (*NIST Draft Special Publication 800-150 - Guide to Cyber Threat Information Sharing)*

Congress.Gov https://www.congress.gov/bill/114th-congress/senate-bill/754/text (Cybersecurity Information Security Act)

Department of Homeland Security (DHS) https://www.dhs.gov/isao *(Information Sharing and Analysis Organizations)*