Government Health Agencies Release Cybersecurity Guidelines

PUBLISHED ON
February 15, 2019

Last month, the Healthcare and Public Health Sector Coordinating Council, a government-backed coalition of hospitals and medical device manufacturers, released a "Medical Device and Health IT Joint Security Plan." The plan outlines protections device manufacturers should take (and hospitals should demand) to reduce exposure to cyber hacking.

This follows the recent release of the "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients," from the Department of Health and Human Services, in partnership with the Health Sector Coordinating Council, in December. The four-volume December publication is designed to provide voluntary cybersecurity practices to health care organizations of all types and sizes, ranging from local clinics to large health care systems.

The most recent publication is a result of the Cybersecurity Act of 2015, in which Congress required that a task force "identify the challenges that the healthcare industry faces when securing and protecting itself against cybersecurity threats." The December publication was in response to a mandate set forth by the Cybersecurity Act of 2015, to develop practical cybersecurity guidelines to cost-effectively reduce cybersecurity risks for the health care industry.

The release of these guidelines follows the recent breach in 2015 to the health insurer Anthem (where the data of nearly 80 million people was compromised) and the 2017 wave of ransomware attacks at 16 British hospitals that forced emergency patient care to be diverted elsewhere. The continuous technological advances of the health care industry make it significantly susceptible to potential compromise of data and medical devices themselves. Nearly all medical equipment and devices are or have the capability of connecting to the internet. The development and widespread use of personal health devices imbedded with software that are or can be used for medical purposes has added to the medical and health information that is susceptible to a cyberattack. The three major threats in the health industry are:

- That a medical device will not perform as intended with the potential to cause significant harm, i.e. pacemaker malfunctions.
- Protected health information is breached or, accessed, possibly leading to improper use.
- Providers receive inaccurate health information, which may lead to improper diagnoses and recommended treatment.

A highly experienced compliance consultant for medical device manufacturers recently explained that the U.S. Food and Drug Administration regulates post-market devices by enabling manufacturers to take design action when a threat becomes apparent without requiring that an application (510(k)) be filed.

He also explained that for pre market devices, U.S. regulations are lacking in any similar provision that is intended to protect against a cyber-attack. However, the applicable European standard (IEC 62304) requires all medical device manufacturers to have cyber security provisions pertaining to the protection of the devices. This standard provides a framework of software development life cycle processes with activities and tasks necessary for the safe design and maintenance of medical devices.

Even though this standard is not directly enforceable in the U.S., a large majority of manufacturers produce devices that are used in both the U.S. and Europe, and thus choose to apply the European standard to all the devices they manufacture.If you are a health care organization with questions on these competing standards and what you should do to protect your electronic information, pleasereach out to meor anyone in ourHealth Law Industry Group.

:

Elizabeth L. Melamed

Associate

Tel: 717-399-1538

Email: emelamed@barley.com