Healthcare & Public Health Sector Coordinating Council
PUBLIC PRIVATE PARTNERSHIP

Connected Health and Cybersecurity – Advice for the Device

By: Rob Suarez, Vice President and CISO, BD
and Aftin Ross, Senior Project Manager, U.S. FDA

October 23, 2019 – National Cyber Security Awareness Month

Whether we're in the doctor's office for a routine checkup, monitoring our health and heart rate with a wearable device on a morning jog, or having surgery in the operating room, we rarely think about the medical devices with software that are connected to us for medical care being vulnerable to a cybersecurity attack. However, the benefits from rapid advances in the use and capabilities of "connected health" also come with potential risks.

According to the American Hospital Association (AHA), the US is home to 6,210 hospitals, each with 50 to 500 beds and 10-15 networked devices per bed. That means with a total of 931,203 staffed hospital beds across the United States, there are some 14 million connected medical devices in the US - just at the bedside, many of which must be protected against cyber-attack and other threats and vulnerabilities. Thus, it is evident that patient safety depends on cyber safety.

This fact is acutely on the minds of both healthcare providers who manage the devices, and medical technology and health I.T. companies who manufacture them. Certain principles are understood when we think about healthcare cyber security: 1) because the threat landscape is constantly evolving, network and device security have difficulty keeping up; 2) healthcare institutions do not have the time, money or resources to independently fix cyber vulnerabilities; 3) patching for updates and vulnerabilities in the medical device ecosystem can be more complicated than your average IT update because there may be a human, not an app, connected to that device and "system reboot" may not be an option; and 4) there are limits in the ability of government regulation to achieve the balance of innovation, effectiveness, security and privacy. It is recognized that these challenges are a shared responsibility and the public and private sector are working together to address these healthcare cybersecurity challenges in various ways.

The Health Sector Coordinating Council (HSCC) – a public private partnership of health sector and government stakeholders dedicated to strengthening the nation's critical healthcare infrastructure against all hazards - convenes these interdependent stakeholders to improve the security and resiliency across the healthcare ecosystem. An HSCC task group addressed the medical device security issue head-on, working over 18 months to publish in January of this year a best practices guide for medical technology companies – the Medical Device and Health I.T. Joint Security Plan (JSP).

The JSP utilizes "security by design" principles throughout the product lifecycle of medical devices and health I.T. solutions. It encourages shared responsibility in the adoption of security related standards, risk assessment methodologies and vulnerability reporting requirements to improve information sharing between manufacturers and healthcare organizations. The JSP is a living document and will be updated as appropriate to adapt to the ever-changing threat environment for medical devices and health I.T. solutions. More follow-on thought is now being given to how hospitals, device manufacturers and government can coordinate how we communicate with patients about device vulnerabilities and security, and how we can deal with the challenging issue of aging medical technologies that have

reached the end of its supported life – whether for security or operational efficiency – but are not easily replaced because of tremendous expense.

These and other critical issues are being addressed in sector-wide workstreams, such as:

- HSCC resource for health providers called the Health Industry Cybersecurity Practices (HICP)
- the FDA's September 10, 2019 Patient Engagement Advisory Committee, which sought to understand how best to communicate cybersecurity risks in health risk communications to patients
- efforts to define and operationalize the imperative for "software bills of materials" to help health systems understand which software components are in the devices and systems they purchase and hence how to manage associated risk
- expansion of the annual DefCon Biohacking Village Device Hacking Lab, where hackers, healthcare providers and device manufacturers collaborate to identify vulnerabilities; and
- the International Medical Device Regulators Forum cybersecurity working group, made up of industry and regulators and co-led by FDA and Health Canada, which is seeking to promote a globally harmonized approach to medical device cybersecurity via drafting of a cybersecurity guide which is available for public comment through December 2, 2019.

We see all these collaborations as signs of significant progress. In 2017, a health care cyber security task force of industry and government leaders diagnosed that healthcare cybersecurity is in "critical condition." The good news is that we have had no reports that cyber incidents involving medical devices have led to direct patient harm to date. However, recognizing that patient safety depends on cyber safety, we have a shared responsibility for robust cyber hygiene and a proactive approach. The work and tools highlighted in this blog are all a part of a coordinated, proactive approach to the cyber safety of medical technologies.

Rob Suarez and Aftin Ross are co-chairs of the Medical Device Security Task Group of the Health Sector Coordinating Council Joint Cybersecurity Working Group