Kim Stanger

Partner
208.383.3913
Boise
kcstanger@hollandhart.com

New FDA Guidance Addresses Medical Device Cybersecurity for the Internet of Things

Insight — 1/05/2017

In 2017, numerous cybersecurity concerns relating to the Internet of Things (“IoT”) will emerge. IoT “refers to the ability of everyday objects to connect to the Internet and to send and receive data.” The network of “things” embedded with electronics, software, and sensors designed to exchange data is expected to grow to at least 50 billion by 2020.

Modern medical devices – such as pacemakers, insulin pumps, and defibrillators – use software and are connected to the networks of hospitals and other health care organizations. As a result, the safety and effectiveness of essential medical devices can be vulnerable to cybersecurity threats from sophisticated hackers – jeopardizing the health of dependent users. Indeed, a report released in August 2016 controversially asserted that pacemakers could be hacked and caused to malfunction.

In today's world, cybersecurity threats are real, ever-present, and continuously changing. The protection of connected medical devices from cybersecurity threats involves continuous maintenance throughout the product's lifecycle, not just during development. Without proper care, post-market innovations, features, and updates that improve a device's function over time can inadvertently open the door to cybersecurity risks.

Final guidance issued December 28 by the Food and Drug Administration, titled “Postmarket Management of Cybersecurity in Medical Devices,” addresses the issue of continuous post-market management of such cybersecurity risks – to ensure that devices remain secure after they are put to use. In addition, the guidance clarifies when software updates to address cybersecurity vulnerabilities must be reported to the FDA – slowing down potential remedies – and when this step can be omitted.

The new guidance is very close to the draft guidance released in January 2016.

In light of the new guidelines, medical device manufacturers should implement a structured and comprehensive program to manage cybersecurity risks. Among other things, manufacturers should:

- Have a way to monitor and detect cybersecurity vulnerabilities in their devices;
- Understand, assess, and detect the level of risk a vulnerability poses to patient safety;

- Establish a process for working with cybersecurity researchers and other stakeholders to receive information about potential vulnerabilities;
- Deploy mitigations such as software patches to address cybersecurity issues early, before they can be exploited and cause harm; and
- Provide implementation guidance to medical professionals deploying the devices in patient settings.

In short, device manufactures must learn to behave less like traditional device makers and more like software designers. The new guidance applies to all medical devices, including those already out on the market.

To answer questions on the guidance, the FDA will hold a January 12, 2017 webinar. For customized advice regarding cybersecurity and data breach preparedness and, please contact C. Mathew Sorensen, Patricia Dean, Kim D. Stanger, or Romaine C. Marshall at Holland & Hart.
