FDA Holds October Workshop to Catalyze Collaborative Approach to Healthcare and Medical Device Cybersecurity; Seeks Comment from Interested Parties

Kristi L. Wolff

October 30, 2014

On October 21-22, 2014, the Food and Drug Administration (FDA) hosted a public workshop on health-related cybersecurity issues. The workshop was entitled “Collaborative Approaches for Medical Device and Healthcare Cybersecurity” and was designed to identify barriers to collaboration in cybersecurity, discuss best practices for countering contemporary risks to critical healthcare infrastructure, and catalyze cooperative development of cyber defense analytical tools and processes.

Building upon the workshop, the FDA announced that it is seeking public comment on medical device security issues. Individuals and organizations concerned with healthcare and medical device-related cybersecurity issues can file comments with the FDA until November 24, 2014.

FDA is the latest federal agency to wade into cybersecurity and critical infrastructure issues in the wake of President Obama’s Cybersecurity Executive Order and the release of the National Institute of Standards and Technology (NIST) Cybersecurity Framework 1.0 (the “Framework”).

Background: Government and Industry Sharpen Focus on Cyber

In February 2013, President Obama issued Executive Order 13636, “Improving Critical Infrastructure Cybersecurity,” and subsequent Presidential Policy Directive 21, charging federal government entities with strengthening cyber defenses, identifying and disrupting threats, and mitigating the consequences of attacks and infiltrations. Among other things, the executive order directed NIST to develop a voluntary framework to promote best practices for cyber readiness.

After a public comment period with significant input from industry, NIST released the first version of its Framework on February 12, 2014. Since its introduction, the Framework has become a foundation protocol for other government agencies working to implement additional guidelines and practices in response to the unique demands of their mandates. As explained below, the FDA has signaled that it will take a similar approach with respect to the cybersecurity of healthcare and medical devices.

The FDA is the latest of many federal agencies and organizations to venture into the cyber ecosystem. The Federal Communications Commission (FCC), the Federal Trade Commission (FTC), the Securities and Exchange Commission (SEC), the Federal Energy Regulatory Commission (FERC), and the General Services Administration (GSA) all spearhead cyber initiatives in their respective spheres. Indeed, the FDA's intent to launch a collaborative approach to cybersecurity in the medical devices and healthcare sectors parallels a similar approach currently underway at the FCC, which recently announced a “new paradigm” for cybersecurity readiness in the communications industry.

Wading In: The Text of the Notice

Along with the Department of Health and Human Services (HHS) and the Department of Homeland Security (DHS), the FDA is seeking to use the workshop and comment period to gather “broad input from the Healthcare and Public Health (HPH) Sector on medical device and healthcare cybersecurity as a way to catalyze collaboration among all HPH stakeholders.”

The objectives of the collaborative model that the FDA aims to construct are twofold: (1) “to incentivize businesses to adopt best practices and industry standards to be included in product design and systems architecture,” and (2) “to foster stakeholder collaboration such that emerging threat and vulnerability information is readily shared.” The initiative's ultimate goal is to “facilitate a forum to implement HPH cyber vulnerability and threat management.”

At the workshop, White House Cybersecurity Coordinator Michael Daniel urged device manufacturers to treat cybersecurity as an essential, integral aspect of product development and design. Daniel drew a comparison between the incorporation of electrical safety features in household appliances and inclusion of cybersecurity features in medical devices: “I think we're going to have to apply a lot of the same principles we have learned in the [electrical] safety area into the cybersecurity area.”

Kevin McDonald, Director of Clinical Information Security at the Mayo Clinic, another speaker at the FDA workshop commented: “I think everyone has a role to play, but frankly, everyone needs to step up. That's what we're not seeing so far.”

The workshop coincided with the Department of Homeland Security announcing that it was opening an investigation into two dozen cases of cybersecurity flaws in medical devices and hospital equipment.

Interested parties may file comments on cybersecurity issues on or before November 24, 2014. Medical device manufacturers, healthcare providers and healthcare app developers should consider the impact of the FDA workshop on their business plans. Kelley Drye is available to assist parties wishing to comment in the proceeding.

Healthcare Cybersecurity To Remain in Focus

The FDA workshop coincides with the proliferation of connected devices increasingly involves medical or fitness trackers targeted at the average consumer. These devices present significant privacy and security issues that regulators will likely address. According to a recent article, personal health credentials sell for between ten and twenty times the value of a U.S. credit card number. Moreover, according to an annual survey conducted by the Ponemon Institute, a cybersecurity think tank, 40% of healthcare organizations suffered a cyber-attack in 2013, up from 20% in 2009. Much of the healthcare industry still relies on outmoded IT systems, which make these organizations especially vulnerable to system infiltration and data theft.

In the healthcare sector, exploited cyber vulnerabilities could cause medical device malfunction, systemic IT infrastructure failures resulting in the interruption of treatment, and inappropriate access to confidential patient information, among other negative consequences.

Moreover, sophisticated medical devices are no longer only available in hospitals and care provider offices but are increasingly accessible to consumers. Popular consumer health apps and devices, such as FitBit, collect massive amounts of data about their users, making them desirable targets for hackers. Many such products also restrict consumer choice with regard to data storage and tracking while implementing minimal security procedures.

Federal legislators and regulators are beginning to take notice. For example, Senator Charles Schumer (D-NY) has called for the FTC to implement new rules and regulations requiring companies to give consumers greater control of the data collected by their apps and devices – including restricting the sale of personal data to certain parties or opting out of data collection altogether. Moreover, according to a recent Politico article, some regulators and lawmakers believe that the new breed of consumer health devices, which fall outside the purview of HIPAA as well as other healthcare regulations, should be regulated in the same stringent manner as other medical devices are now. Finally, last November the FTC held an all-day workshop on the Internet of Things, with a particular focus on privacy and security concerns.

In all, this federal activity heralds an increasing focus on cybersecurity and consumer privacy, which likely will have a significant impact on businesses in the medical industry and Internet of Things space that collect and use consumer data. Businesses in this area should closely monitor developments at the federal agencies and on Capitol Hill.

TeleHealth and the Internet of Things at Kelley Drye

Kelley Drye attorneys regularly navigate the myriad and overlapping regulations governing the operation of interconnected devices generally and medical and healthcare devices and software in particular. Our experience ranges from advising clients on FDA regulation of medical IT systems to ensuring that medical devices properly comply with privacy and data security obligations, including, but not limited to, FTC guidelines and state-level regulations.

Moreover, please be advised that attorneys in Kelley Drye & Warren’s Communications Practice Group are experienced in addressing cybersecurity compliance issues and are able to assist clients in navigating such issues. For additional information, contact Kristi Wolff,.

Please contact us if you are interested in filing comments.