FDA Seeks to Catalyze Collaborative Approach to Healthcare and Medical Device Cybersecurity; Announces October Workshop and Comment Deadlines

Kristi L. Wolff

September 29, 2014

On September 23, 2014, the Food and Drug Administration (FDA) released a notice of public workshop and request for comments on health-related cybersecurity issues in the Federal Register. Per the announcement, on October 21 and 22, the FDA will host a two-day public workshop entitled "Collaborative Approaches for Medical Device and Healthcare Cybersecurity," which is 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. The workshop will also be available via webcast. Following the event, the FDA will accept comments related to workshop subject matter.

With the announcement, the FDA becomes 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.

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."

The public notice describes a number of topics that will be discussed at the workshop including:

- Fostering a collaborative environment for information sharing and the development of a shared risk-assessment framework using a common lexicon;
- Overcoming barriers (both perceived and real) to creating a community of "shared ownership and shared responsibility" within the HPH Sector;
- Increasing situational awareness of the current cyber threats to the sector, especially to medical devices, and identifying cybersecurity gaps and challenges, with particular attention to end-of-life support for legacy devices and interconnectivity of medical devices;
- Adapting and implementing the NIST Framework to support management of cybersecurity risks involving medical devices;
- Developing tools and standards to build a comprehensive cybersecurity program to meet the unique needs of the sector's critical infrastructure; and
- Leveraging the technical subject matter expertise of the cybersecurity researcher community and working with HPH stakeholders to identify, assess, and mitigate vulnerabilities as well as collaborate in building adaptive and robust solutions to current problems.

Comments are due November 24, 2014. Individuals and organizations need not attend the workshop to file comments. The workshop will be held at the National Intellectual Property Rights Coordination Center Auditorium in Arlington, Virginia.

Widespread Agency Involvement in Cybersecurity

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.

The FDA's announcement comes at an important time, as 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. For this reason, 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,.

More Event Details:

To register for the public workshop and to view additional information about the evern, please visit FDA’s Medical Devices News & Events—Workshops & Conferences calendar at http://www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/default.htm (Select this public workshop from the posted events list.

See the Federal Register Notice for more information.