KING & SPALDING

Client Alert

Data, Privacy & Security Practice Group

October 24, 2014

FDA Issues Cybersecurity Guidelines

Manufacturers of Medical Devices Encouraged to Develop Cybersecurity Controls

The Food and Drug Administration (FDA) issued guidelines this month recommending that manufacturers develop a set of cybersecurity controls in the design of medical devices capable of connecting to the Internet, a network, or portable media.[1] Manufacturers should not only identify the cybersecurity risks associated with the device, but also develop a way for the appropriate stakeholders to detect and respond to security compromises.[2]

The purpose of the guidelines is to ensure the functionality and safety of medical devices from intentional or unintentional cybersecurity risks.[3] While interconnected devices can improve patient care and create healthcare efficiencies, they are vulnerable to security breaches.[4] The FDA's cybersecurity concerns include malware infections that can spread over networks to medical devices, unsecured distribution of passwords, untimely software updates and patches, and security vulnerabilities in off-the-shelf software.[5]

Though the guidelines are recommendations that do not have the force of law,[6] the FDA has made clear that it will use these guidelines in clearing medical devices for commercial distribution. Failure by medical device companies to comply with the guidelines and adequately describe the cybersecurity measures implemented in the device may delay or even prevent the FDA from approving a premarket application.

The FDA guidelines provide direction for how medical device companies should document cybersecurity measures for premarket submissions of medical devices. Documentation should include a list of the cybersecurity risks the manufacturer considered in the design of the device, a list of the cybersecurity controls incorporated in the device, justifications for how the controls respond to the risks, and a plan for how to validate software updates and patches.[7] These documentation requests highlight the importance of considering security measures during the design of a medical device and not as an afterthought.

The FDA's guidelines recognize the need to balance security measures with usability of the device in the design of security controls. The controls should account for the unique usability challenges of a health care setting

For more information, contact:

Phyllis B. Sumner
+1 404 572 4799
psumner@kslaw.com

Sarah E. Statz
+1 404 572 2813
sstatz@kslaw.com

Kerianne Tobitsch
+1 212 556 2310
ktobitsch@kslaw.com

King & Spalding
Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521
Tel: +1 404 572 4600
Fax: +1 404 572 5100

www.kslaw.com

where unauthorized users may need to access a medical device, such as when an emergency room physician without prior authorization needs immediate access to a patient's device.[8] One suggestion is to use a layered authorization model with differentiated privileges for different users.[9] The FDA also recommends that hospitals and other health care facilities evaluate the security of their networks and implement ways to protect the hospital system.[10] Common forms of cyber protection, such as hardcoded passwords in which each device has the same password, leave devices vulnerable to hacking if the hospital is using an unsecured network.[11]

The issuance of these guidelines highlights the need for medical device manufacturers and health care facilities to think about cybersecurity as an integral part of providing health care. The FDA's decision to release these guidelines, despite no indication that certain devices or systems have been targeted and no known harm to patients from security breaches,[12] demonstrates the need for manufacturers and health care facilities to take proactive measures to protect patients from cybersecurity risks. As manufacturers design and develop new medical devices, they should identify risks based on the intended use and intended environment for the devices[13] so that they can develop tailored cybersecurity controls. Manufacturers and health care facilities should also test existing devices and networks for cyber vulnerabilities and provide software updates and patches as needed.

King & Spalding's Data, Privacy and Security Practice

King & Spalding is particularly well equipped to assist clients in the area of privacy and information security law. Our Data, Privacy & Security Practice regularly advises clients regarding the myriad statutory and regulatory requirements that businesses face when handling personal customer information and other sensitive information in the U.S. and globally. This often involves assisting clients in developing comprehensive privacy and data security programs, responding to data security breaches, complying with breach notification laws, avoiding potential litigation arising out of internal and external data security breaches, defending litigation, whether class actions brought by those affected by data breaches, third party suits, or government actions, and handling both state and federal government investigations and enforcement actions.

With more than 30 Data, Privacy & Security lawyers in offices across the United States, Europe and the Middle East, King & Spalding is able to provide substantive expertise and collaborative support to clients across a wide spectrum of industries and jurisdictions facing privacy-based legal concerns. We apply a multidisciplinary approach to such issues, bringing together attorneys with backgrounds in corporate governance and transactions, healthcare, intellectual property rights, complex civil litigation, e-discovery, government investigations, government advocacy, insurance recovery, and public policy.

* * *

This alert provides a general summary of recent legal developments. It is not intended to be and should not be relied upon as legal advice. In some jurisdictions, this may be considered "Attorney Advertising."

[1] DEPARTMENT OF HEALTH AND HUMAN SERVICES, FOOD AND DRUG ADMINISTRATION, Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, Guidance for Industry and Food and Drug Administration Staff, (Oct. 2, 2014), *available at* http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf [hereinafter "FDA Guidance"].

[2] FDA Guidance at 4-5.
[3] FDA Guidance at 2-3.
[4] Press Release, “The FDA Takes Steps to Strengthen Cybersecurity of Medical Devices” (Oct. 1, 2014), *available at* http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm416809.htm [hereinafter “Press Release”].
[5] Press Release.
[6] FDA Guidance at 2.
[7] FDA Guidance at 6.
[8] *See* FDA Guidance at 4; *see also* Robert Lemos, *Medical Device Cybersecurity Necessary*, *But Optional*, (Oct. 6, 2014), Ars Technica, *available at* http://arstechnica.com/security/2014/10/fda-medical-device-cybersecurity-necessary-but-optional/ [hereinafter “Lemos article”].
[9] FDA Guidance at 5.
[10] Food and Drug Administration, Cybersecurity, *available at* http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/ConnectedHealth/ucm373213.htm (last updated Oct. 8, 2014).
[11] FDA Guidance at 5, *see also* Lemos article.
[12] Press Release.
[13] FDA Guidance at 4.