KING & SPALDING

Client Alert

Data, Privacy & Security, FDA & Life Sciences, and Tort Practice Groups

January 26, 2016

FDA Issues Draft Guidance Governing Postmarket Cybersecurity Risk Management Standards

On January 15, 2016, the U.S. Food and Drug Administration (FDA) announced in a Press Release that it would issue draft guidance on January 22 outlining "steps medical device manufacturers should take to continually address cybersecurity risks" to confront "vulnerabilities in medical devices once they have entered the market." FDA published a Notice in the Federal Register on January 22 and has requested public comments within 90 days, by April 20, 2016. FDA's Draft Guidance on Postmarket Management of Cybersecurity in Medical Devices itself can be found **here**. FDA issued this guidance in advance of a public workshop, entitled "Moving Forward: Collaborative Approaches to Medical Device Cybersecurity" that was webcast and archived on FDA's website.

This new postmarket draft guidance builds on FDA's October 2014 "nonbinding" cybersecurity guidance that encouraged medical device manufacturers to develop and incorporate cybersecurity controls into medical devices at the premarket design stage. Our prior coverage of FDA's 2014 action can be found **here**. As was the case in October 2014, FDA bills this new postmarket cybersecurity draft guidance as "not binding on FDA or the public" and states that regulated entities may use "an alternative approach [to cybersecurity risk management] if it satisfies the requirements of the applicable statutes and regulations." That said, FDA's most recent draft guidance makes clear that it will employ its enforcement resources to police cybersecurity issues in marketed medical devices where a known cybersecurity vulnerability seriously impacts public health.

Highlights of FDA's Draft Guidance on Postmarket Management of Cybersecurity in Medical Devices

FDA's draft guidance applies to: (i) medical devices that contain software (including firmware) or programmable logic, and (ii) software that is a medical device. However, it is not intended to cover experimental or investigational medical devices. Consistent with its October 2014 guidance, FDA's newest pronouncement on cybersecurity for medical devices relies heavily on President Obama's Executive Orders on cybersecurity issues and the National Institute of Standards and Technology (NIST) voluntary Cybersecurity Framework.

For more information, contact:

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

Mark S. Brown
+1 202 626 5443
mbrown@kslaw.com

D. Fritz Zimmer
+1 415 318 1220
fzimmer@kslaw.com

Elaine Tseng
+1 415 318 1240
etseng@kslaw.com

Alexander K. Haas
+1 202 626 5502
ahaas@kslaw.com

Cameron Hoyler
+1 213 443 4350
choyler@kslaw.com

King & Spalding
Washington, D.C.
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4707
Tel: +1 202 737 0500
Fax: +1 202 626 3737

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

www.kslaw.com

Information Sharing. FDA describes cybersecurity as a "shared responsibility" of "the medical device manufacturer, the user, the Information Technology (IT) system integrator, Health IT developers, and an array of IT vendors that provide products that are not regulated by the FDA." FDA seeks to promote "a culture of cybersecurity risk management" and collaboration through information sharing "to leverage available resources and tools to establish a common understanding that assesses risks for identified vulnerabilities in medical devices among the information technology community, healthcare delivery organizations (HDOs), the clinical user community, and the medical device community." To that end, FDA's draft guidance encourages the sharing of cyber risk information and intelligence within the medical device community by creating incentives for industry to join Information Sharing Analysis Organizations (ISAOs). While participation in these ISAOs is voluntary, FDA's draft guidance suggests that it will favorably look upon medical device manufacturers that belong to these organizations by, for example, not enforcing certain reporting requirements of the Federal Food, Drug, and Cosmetic Act and through its enforcement decisions.

Continually Evolving Risks and "Critical Components" of a Cybersecurity Surveillance Program. FDA recognizes that "medical devices and the surrounding network infrastructure cannot be completely secured." Likewise, FDA agrees with the proposition that it is "not possible" to completely mitigate risks through premarket controls and cybersecurity-by-design. As a result, it is "essential" for manufacturers of medical devices to "implement comprehensive cybersecurity risk management programs and documentation" as required in a host of FDA requirements contained in the Quality System Regulation (21 CFR Part 820). Thus, while "non-binding," this guidance is a tipoff that regulatory investigations and potential enforcement actions could follow if FDA concludes that a medical device does not meet its Quality System Regulation. The focus of a medical device manufacturer's postmarket program should be on "unauthorized access, modification, misuse or denial of use, or the unauthorized use of information that is stored, accessed, or transferred from a medical device to an external recipient" that may impact patient safety. FDA's draft guidance indicates that "critical components" of a cybersecurity surveillance program include:

- Monitoring cybersecurity information sources for identification and detection of cybersecurity vulnerabilities and risk;
- Understanding, assessing and detecting presence and impact of a vulnerability;
- Establishing and communicating processes for vulnerability intake and handling;
- Clearly defining essential clinical performance to develop mitigations that protect, respond and recover from the cybersecurity risk;
- Adopting a coordinated vulnerability disclosure policy and practice; and
- Deploying mitigations that address cybersecurity risk early and prior to exploitation.

The management of these risks will require the medical device manufacturer to have methods to both: (i) identify, characterize, and assess a cybersecurity vulnerability; and (ii) analyze, detect, and assess threat sources, including within the manufacturer's supply chain and among third-party vendors. FDA "recommends" that manufacturers "incorporate[] elements consistent with" the NIST Cybersecurity Framework.

Medical Device Cybersecurity Risk Management. A medical device manufacturer must define the essential clinical performance of a medical device as part of its assessment of the device's vulnerability to cybersecurity risks. FDA's draft guidance states that "a manufacturer should establish, document, and maintain throughout the medical device lifecycle an ongoing process for identifying hazards associated with the cybersecurity of a medical device, estimating and evaluating the associated risks, controlling these risks, and monitoring the effectiveness of the controls." With this information in hand, one can assess risk to a medical device's essential clinical performance by looking at two factors: (i) the exploitability of the cybersecurity vulnerability, and (ii) the severity of the health impact to patients if the vulnerability were to be exploited. Evaluating this risk will lead to a conclusion that a cyber-risk is "controlled (acceptable) or uncontrolled (unacceptable)." FDA's draft guidance provides recommendations for addressing and

reporting risks that differ in part based on whether the risk is controlled or uncontrolled. The draft guidance also includes a proposed matrix that compares the exploitability of the vulnerability in the medical device to the severity of the impact to public health as an "example" of how to "assess the risk to [a] device's essential clinical performance from a cybersecurity vulnerability as controlled or uncontrolled" (shown below):

Remediation, Reporting, and the Threat of Investigations and Enforcement Actions. FDA's draft guidance encourages "efficient, timely and ongoing" cybersecurity risk management for marketed devices and, in particular, the remediation of identified cybersecurity risks. Notably, FDA "typically" will not require premarket review of "routine updates and patches" for clearance or approval. However, medical device manufacturers must, among other things, conduct appropriate software validation under FDA regulations, properly document their methods and controls, and "[p]rovide users with relevant information on recommended work-arounds, temporary fixes and residual cybersecurity risks" to ensure appropriate mitigation. Significantly, FDA's draft guidance offers examples of the mitigation of controlled risks and uncontrolled risks, including FDA's current thinking on whether cybersecurity changes require formal FDA reporting in various contexts. Of particular note is that FDA asserts that vulnerabilities associated with uncontrolled risks "must" be remediated, and that in the "absence of remediation" FDA may consider the product to be "in violation of the FD&C Act and subject to enforcement and other action."

FDA Seeks Comments on Five Specific Questions

In addition to comments on its draft guidance generally, FDA's Notice in the Federal Register also has sought comments on the following five specific questions:

- What factors contribute to a manufacturer's decision whether or not to participate in an ISAO?
- In the draft guidance, FDA is proposing its intention to not enforce certain regulatory requirements for manufacturer's that are "participating members" of an ISAO. Should FDA define what it means to be a "participating member" of an ISAO and if so, how should such participation be verified?
- What are the characteristics (participation, expertise, policies, and practices) of an ISAO that would make it qualified to participate in the sharing and analysis of medical device cybersecurity vulnerabilities? What are the benefits and disadvantages of FDA "recognizing" specific ISAOs as possessing specialized expertise relevant to sharing and analysis of medical device vulnerabilities and what should such recognition entail?

- When cybersecurity vulnerability information is not reported to FDA, what information should be reported to the ISAO, and when?
- How should FDA interact with ISAOs, manufacturers, HDOs, security researchers and other stakeholders to maximize the sharing of information concerning cybersecurity threats while maintaining confidentiality and protecting commercial confidential information?

FDA will be accepting comments on the draft guidance for a 90-day period ending April 20, 2016. We recommend that medical device manufacturers subject to FDA oversight carefully consider the implications imposed by the draft guidance and consider submitting comments.

Recommendations

As FDA's draft guidance shows, many agencies of the U.S. Government continue to focus on cybersecurity risk management, particularly in cases where public health and safety could be adversely impacted. Moreover, the draft guidance once again indicates how cyber incidents may swiftly escalate to business crises, which can create legal predicaments through regulatory investigations, enforcement actions, and potential litigation. As a result, medical device manufacturers should ensure that they have a means to identify and address potential cybersecurity vulnerabilities in products and find cost-effective means to (i) reduce the likelihood of cyber incidents in medical devices, and (ii) minimize the business and legal impact of such incidents. For example, companies should have a compliance program to monitor these vulnerabilities and consider means to share cyber threat information consistent with the recommendations of FDA in a manner that protects patient privacy.

It is very likely that FDA will issue final guidance in 2016 based on the comments it receives. Likewise, we believe it is likely that FDA will, at some point, investigate publicly reported cybersecurity incidents involving medical devices and could institute enforcement actions in the right case. Notably, in July 2015, FDA issued its first Safety Alert publicly warning hospitals against the purchase and use of a medical device (an infusion pump) associated with "cybersecurity vulnerabilities" that "could lead to over- or under-infusion of critical patient therapies." Having a documented and established compliance program to mitigate cybersecurity risk will help avert or minimize the impact of future FDA investigations and enforcement actions prompted by cybersecurity concerns. King & Spalding will continue to monitor developments with regard to FDA's focus on the cybersecurity of medical devices and will provide updates if new regulations or guidelines are issued or if enforcement actions are publicized. We invite you to consult with us further regarding the implications of FDA's actions.

* * *

King & Spalding's Data, Privacy and Security and FDA & Life Sciences Practices

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 in the U.S. and globally when handling personal information and other sensitive information and addressing cybersecurity requirements. 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 60 Data, Privacy & Security lawyers in offices across the United States, Europe, Russia, 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 and data security-based legal concerns.

In addition, in 2015, King & Spalding was named "Law Firm of the Year" for FDA law by U.S. News & World Reports. King & Spalding's FDA & Life Sciences team has more than 30 attorneys and other professionals, who provide practical legal counseling and technical consulting on a full array of issues involving all FDA regulated products, including medical devices. Among other things, our team is experienced in responding to FDA warning letters and FDA-483 observations, conducting audits of quality systems, representing clients before the FDA on enforcement issues, and helping clients submit device marketing applications. We also have significant experience shaping policy at FDA and on the Congressional level.

We apply a multidisciplinary approach to our matters, 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.