**FDA Recommends Medical Device Manufacturers Implement a Comprehensive Cybersecurity Risk Management Program in Accordance with NIST Standards**

By Kim Tyrrell-Knott and Shilpa Prem

February 2016

Medical devices increasingly contain software or connect to networks that may leave the devices vulnerable to cyber-attacks. The U.S. Food and Drug Administration ("FDA") has recognized the potential risks that these cybersecurity vulnerabilities may have on patient safety. In a series of guidances, FDA is emphasizing the need for medical device manufacturers to proactively manage such risks throughout the product life cycle.

On January 15, 2016, FDA released new draft guidance, “Postmarket Management of Cybersecurity in Medical Devices” (“Postmarket Cybersecurity Guidance”), recommending a series of cybersecurity postmarket controls. Previously, in October 2014, FDA published a guidance entitled “Content of Premarket Submissions for Management of Cybersecurity in Medical Devices” (“Premarket Cybersecurity Guidance”). Taken together, these FDA guidance documents provide a framework for medical device manufacturers to create a comprehensive risk management program specifically focused on cybersecurity vulnerabilities of their medical devices that include some type of software or connectivity to networks. Moreover, with such FDA guidance in place, the risks are greater to medical device manufacturers if a cybersecurity breach occurs because these manufacturers failed to create such a risk management program.

---

Premarket Considerations

In its Premarket Cybersecurity Guidance, FDA recommends that medical device manufacturers develop a set of cybersecurity controls to reduce the likelihood that device functionality would be compromised by inadequate security and to maintain the integrity of medical device functionality and safety. As part of a premarket submission, FDA also expects a medical device manufacturer to provide documentation demonstrating how the manufacturer has considered cybersecurity risks and effectively implemented security controls in its device design.

That requirement includes, but is not limited to, establishing design inputs relating to cybersecurity. This also includes a cybersecurity management approach to software validation and a risk analysis as part of the manufacturer's quality system. FDA encourages manufacturers to address the following key elements:

- Identification of assets, threats, and vulnerabilities
- Assessment of the impact of threats and vulnerabilities on device functionality and end users/patients
- Assessment of the likelihood of a threat and of a vulnerability being exploited
- Determination of risk levels and suitable mitigation strategies
- Assessment of residual risk and risk acceptance criteria

While these key elements are similar to risk management processes implemented by medical device manufacturers today, FDA recommends that manufacturers follow five functions with respect to cybersecurity risks set out in the National Institute of Standards and Technology’s “Framework for Improving Critical Infrastructure Cybersecurity” ("NIST Framework").¹ Identify, Protect, Detect, Response, and Recover.

Under the NIST Framework:

- “Identify and Protect” consists of (1) identifying the cybersecurity risks of the medical device when used in connection with the wireless network, the Internet, or other portable media, and (2) appropriately implementing safeguards to protect against such risks. Such protection could include allowing limited access to trusted users through password protection or biometric protections and restricting access to the software to trusted parties. FDA appreciates the impact that these security controls may have on usability

and urges manufacturers to appropriately balance the need for security with efficient use and access given the devices intended use and environment.

- “Detect, Response, and Recover” involves implementing features that allow for security compromises to be detected, recognized, logged, timed, and acted upon during normal use. Manufacturers should consider safeguards that enable critical features of the device to continue to function even if a cybersecurity attack were to compromise the device.

Postmarket Considerations

Given the evolving nature of potential cybersecurity threats, FDA’s Postmarket Cybersecurity Guidance emphasizes the need to continue to monitor, identify, and address potential cybersecurity risks after a device has been released to the market. To effectively monitor cybersecurity threats, it is important to recognize that information regarding cybersecurity vulnerabilities or attacks may come from non-traditional sources. While patient safety risk are traditionally identified through customer complaints, manufacturer investigations, or postmarket surveillance, intelligence about cybersecurity threats may originate from other industry sectors (e.g., finance or defense) or cybersecurity resources outside the medical device arena. These differences need to be taken into account when the manufacturer develops the postmarket elements of its cybersecurity risk management program.

FDA recommends that manufacturers incorporate cybersecurity considerations into the risk management program and apply the NIST Framework to their postmarket cybersecurity risk management program. Although at a high level the risk management recommendations are consistent with standard practices in the medical device industry, there are a number of key differences and additions that manufacturers should note.

FDA recommends that manufacturers evaluate the risk to the device’s “essential clinical performance” and remediate those risks down to an acceptable level. Specifically, under the draft Postmarket Cybersecurity Guidance, manufacturers should examine (1) the exploitability of a cybersecurity vulnerability and (2) the severity of harm to the patient if it were exploited.

This process is similar, in concept, to assessing probability of occurrence and severity of harm in a traditional risk assessment. However, FDA recommends that manufacturers use a cybersecurity vulnerability tool that evaluates a range of new factors. These factors include, for example:

- Attack Vector (physical, local, adjacent, network)
- Attack Complexity (high, low)
- Privileges Required (none, low, high)
- User Interaction (none, required)
FDA also suggests that manufacturers perform threat modeling and an analysis of threat sources. Threat modeling optimizes network, application, or Internet security by identifying potential and actual vulnerabilities and defining countermeasures. Threat modeling is different from traditional medical device risk management in that it provides a framework to assess threats from active adversaries or malicious users, which are common among cybersecurity threats.

Another key addition to the manufacturers’ traditional risk management practices is the recommendation to proactively monitor cybersecurity specific sources in order to identify potential cybersecurity threats or signals. These sources include Computer/Cyber Emergency Response/Readiness Teams (“CERTS”), Information Sharing and Analysis Organizations (“ISAOs”), security researchers, or other critical infrastructure or industries. The early detection of emerging threats will assist manufacturers in timely addressing new exploits that could adversely impact patient safety. FDA also encourages manufacturers to incorporate detection mechanisms into their devices in order to enhance the identification of attacks and assist in exploit forensics.

**Conclusion**

Although FDA’s Postmarket Cybersecurity Guidance is only a draft at this time, it still provides a glimpse into FDA’s current thinking about cybersecurity and the importance of effectively mitigating cybersecurity risks at all stages of the product life cycle. Given the potential threat that cyber-attacks pose to patient safety and the increasing importance of software and network connectivity to medical devices, manufacturers should evaluate their current risk management programs and consider incorporating robust cybersecurity procedures and controls into such programs that are consistent with NIST standards and other cybersecurity best practices. Failure to do so may lead to increased risks if a breach occurs at a later time.

* * *

---

Thought Leaders in Health Law®
This Client Alert was authored by Kim Tyrrell-Knott and Shilpa Prem. For additional information about the issues discussed in this Client Alert, please contact one of the authors or the Epstein Becker Green attorney who regularly handles your legal matters.

This document has been provided for informational purposes only and is not intended and should not be construed to constitute legal advice. Please consult your attorneys in connection with any fact-specific situation under federal law and the applicable state or local laws that may impose additional obligations on you and your company.

About Epstein Becker Green

Epstein Becker & Green, P.C., is a national law firm with a primary focus on health care and life sciences; employment, labor, and workforce management; and litigation and business disputes. Founded in 1973 as an industry-focused firm, Epstein Becker Green has decades of experience serving clients in health care, financial services, retail, hospitality, and technology, among other industries, representing entities from startups to Fortune 100 companies. Operating in offices throughout the U.S. and supporting clients in the U.S. and abroad, the firm’s attorneys are committed to uncompromising client service and legal excellence. For more information, visit www.ebglaw.com.

IRS Circular 230 Disclosure

To ensure compliance with requirements imposed by the IRS, we inform you that any tax advice contained in this communication (including any attachments) is not intended or written to be used, and cannot be used, for the purpose of: (i) avoiding any tax penalty, or (ii) promoting, marketing or recommending to another party any transaction or matter addressed herein.

If you would like to be added to our mailing list or need to update your contact information, please contact Lisa C. Blackburn at lblackburn@ebglaw.com or 202-861-1887.
# HEALTH CARE & LIFE SCIENCES

## BALTIMORE
- Helaine I. Fingold
- Joshua J. Freemire
- Thomas E. Hutchinson*
- John S. Linehan

## BOSTON
- Emily E. Bajcsi
- Barry A. Guryan

## CHICAGO
- Bradley S. Davidsen
- Amy K. Dow
- Mark A. Mosby
- Kevin J. Ryan

## HOUSTON
- Mark S. Armstrong

## LOS ANGELES
- Adam C. Abrahms
- Ted A. Gehring
- Paul A. Gomez
- J. Susan Graham

## NEW YORK
- Jeffrey H. Becker
- Lindsay M. Borgeson
- Michelle Capezza
- Karen L. Cavalli
- Aime Dempsey
- Kenneth W. DiGia
- Charles C. Dunham, IV
- Jerrold I. Ehrlich
- Gregory H. Epstein
- Hanna Fox
- James S. Frank
- Arthur J. Fried
- John F. Gleason
- Robert D. Goldstein
- Robert S. Groban, Jr.
- Gretchen Harders
- Bethany J. Hills
- Carly Eisenberg Hoinacki
- Jennifer M. Horowitz
- Kenneth J. Kelly
- Joseph J. Kempf, Jr.
- Basil H. Kim
- Stephanie G. Lerman
- Leonard Lipsky
- Purvi Badiani Maniar
- Wendy G. Marcari
- Eileen D. Millett
- Shilpa Prem
- Jackie Selby
- Victoria M. Sloan
- Steven M. Swirsky
- Benjamin T. Tso
- David E. Weiss
- Alison M. Wolf*
- Benjamin M. Zegarelli

## NEWARK
- John D. Barry
- Christina Burke
- Joan A. Dieler
- James P. Flynn
- Diana M. Fratto
- Gary W. Herschman
- Laurajane B. Kastner
- Daniel R. Levy
- Theodora McCormick
- Maxine Neuhauser
- Anjana D. Patel
- Victoria Vaskov Sheridan
- Erica F. Sibley
- Scheherazade A. Wasty
- Jack Wenik
- Sheila A. Woolson

## PRINCETON
- Anthony Argiropoulos
- Thomas Kane
- Andrew Kaplan
- Jeffrey G. Kramer

## SAN DIEGO
- Kim Tyrrell-Knott

## STAMFORD
- Ted Kennedy, Jr.
- David S. Poppick

## WASHINGTON, DC
- Alan J. Arville
- Robert F. Atlas*
- Kirsten M. Backstrom
- Clifford E. Barnes
- James A. Boiani
- George B. Breen
- Lee Calligaro
- Tanya V. Cramer
- Anjali N.C. Downs
- Jason E. Christ
- Steven B. Epstein
- John W. Eriksen
- Wandalay E. Fernández
- Daniel C. Fundakowski
- Brandon C. Ge
- Stuart M. Gerson
- Daniel G. Gottlieb
- M. Brian Hall, IV
- Philo D. Hall
- Douglas A. Hastings
- Jonathan K. Hoerner
- Robert J. Hudock
- Richard H. Hughes IV
- William G. Kopf
- Amy F. Lerman
- Wenxi Li*
- Christopher M. Locke
- Katherine R. Loftt
- Mark E. Lutes
- Teresa A. Mason
- David E. Matyas
- Colin G. McCulloch
- Frank C. Morris, Jr.
- Leslie V. Norwalk
- René Y. Quashie

Jonah D. Retzinger
Serra J. Schlanger
Bonnie I. Scott
Deepa B. Selvam
Lynn Shapiro Snyder
Adam C. Solander
James S. Tam*
David B. Talge
Daly D.E. Temchine
Bradley Merrill Thompson
Carrie Valiant
Patricia M. Wagner
Robert E. Wanerman
Meghan F. Weinberg
Constance A. Wilkinson
Kathleen M. Williams
Lesley R. Yeung

*Not Admitted to the Practice of Law

© 2016 Epstein Becker & Green, P.C.  Attorney Advertising