DRUG AND DEVICE BULLETIN

FEBRUARY 12, 2016

SHOOK
HARDY & BACON

FDA ISSUES DRAFT GUIDANCE ON POSTMARKET CYBERSECURITY PROGRAMS FOR MEDICAL DEVICES

In 2014, the U.S. Food and Drug Administration (FDA) articulated its expectations for the ways device manufacturers should address cybersecurity premarket in *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*. More recently, FDA released complementary draft guidance in *Postmarket Management of Cybersecurity in Medical Devices*. In the new guidance, the agency explains what constitutes an effective cybersecurity risk management program, how manufacturers should evaluate postmarket cybersecurity vulnerabilities, and when manufacturers must report cybersecurity risks and improvements to FDA. Comments about the draft guidance are due by April 21, 2016.

Key takeaways from the guidance include:

- Cybersecurity programs should be documented, systematic and comprehensive.
- Cybersecurity should be considered throughout the medical device's entire lifecycle.
- Cybersecurity evaluations should consider a broad range of credible information and potential threats that could compromise a medical device's essential functions.

Components of an Effective Cybersecurity Risk Management Program

The new guidance exhorts manufacturers to create a cybersecurity risk management program that will address a device's cybersecurity from the drawing board to the dustbin.

Manufacturers should account for cybersecurity by designing cybersecurity-related inputs for their devices and incorporating a cybersecurity management approach that determines (1) assets, threats and vulnerabilities; (2) how threats and vulnerabilities could affect device functionality

Shook offers expert, efficient and innovative representation to clients targeted by litigation and regulation. By partnering with companies to navigate the complex operational, technological and regulatory challenges of today's global business environment, we are able to manage emerging threats and overcome potential obstacles at every step in the decision-making process.

For more information about this issue of the Drug and Device Bulletin, please contact:

Al Saikali
Partner | Miami
305.358.5171
asaikali@shb.com

Madeleine McDonough
Partner | Washington, D.C.
202.639.5600
mmcdonough@shb.com

Tim Moore
Senior Associate | Miami
305.755.8924
tmoore@shb.com

and end users/patients; (3) the likelihood of threats and exploitation of vulnerabilities; (4) risk levels and suitable mitigation strategies; and (5) residual risk and risk acceptance criteria. FDA provided the same recommendations in its 2014 premarket guidance.

Adequate postmarket cybersecurity management requires a program that is systematic, structured, documented, consistent with the Quality System Regulation (21 C.F.R. Part 820), and incorporates the National Institute of Standards and Technology's (NIST's) *Framework for Improving Critical Infrastructure Cybersecurity* (cybersecurity guidelines NIST created pursuant to a presidential executive order and with input from public and private stakeholders).

Key components include:

- monitoring quality cybersecurity information sources—such as complaints, service records and data provided through Information Sharing Analysis Organizations (ISAOs)—for identification and detection of vulnerabilities and risk;
- establishing, communicating and documenting processes for vulnerability intake and handling;
- understanding, assessing and detecting the presence and impact of vulnerabilities;
- clearly defining essential clinical performance to develop mitigations that protect, respond and recover from cybersecurity risk;
- adopting a coordinated vulnerability disclosure policy and practice; and
- deploying mitigations that address cybersecurity risk early and before exploitation.

Assessing Postmarket Cybersecurity Vulnerabilities

Acknowledging that not all vulnerabilities threaten patient safety and that manufacturers may not be able to identify every threat, the guidance advises manufacturers to identify a device's "essential clinical performance" and focus on identifying and resolving risks to that performance. Manufacturers should define a device's essential clinical performance by considering the conditions necessary for the device to operate safely and effectively. Manufacturers should assess a vulnerability's risk by evalu-

ating its exploitability and health dangers resulting from its exploitation. The draft guidance recommends tools for each evaluation: the *Common Vulnerability Scoring System v3.0* for exploitability and the standards in *ANSI/AAMI/ISO 14971: 2007/(R)2010: Medical Devices – 442 Application of Risk Management to Medical Devices* for health dangers caused by exploitation.

The guidance divides risks into two groups and recommends manufacturers do the same. Low or "controlled" risk exists when, after accounting for existing controls, there is an acceptable amount of risk that the device's essential clinical performance could be compromised by a cybersecurity vulnerability. High or "uncontrolled" risk exists when insufficient controls and mitigations create an unacceptable amount of risk that the device's essential clinical performance could be compromised by a cybersecurity vulnerability.

Reporting Mitigation

A risk's classification affects whether a manufacturer can address the risk without reporting the risk and its remediation to FDA under 21 C.F.R. Part 806, which obligates manufacturers to report when they repair, modify or adjust a device to reduce the device's health risk. Manufacturers can ameliorate controlled risks without reporting the risk or enhancement under Part 806. (But for Class III devices, manufacturers must disclose the risk and the remediation in their periodic reports to FDA under 21 C.F.R. § 814.84.) Uncontrolled risks are a different matter: manufacturers must report them and their remediation unless (1) there are no known serious adverse events or deaths associated with the vulnerability; (2) within 30 days of learning of the vulnerability, the manufacturer identifies and implements device changes and/or compensating controls to bring the residual risk to an acceptable level and notifies users; and (3) the manufacturer participates in an ISAO.

What the Draft Guidance Means for Device Manufacturers

Device manufacturers should not delay assessing the strength of their cybersecurity management program. The U.S. Department of Health and Human Services, Office of Inspector General identified medical device cybersecurity as one of its priorities for 2016. And the draft guidance explains that FDA might consider devices with uncontrolled risk in violation of the FDCA and be subject to enforcement action.

To see how their programs measure up to what the draft guidance describes, device manufacturers should start by asking these key questions:

- Is our cybersecurity management program addressing cybersecurity throughout each device's lifecycle?
- Is our program proactive?
- Should we use quality data security sources, such as ISAOs?
- Do we need to develop and deploy new training or messaging to colleagues about cybersecurity?
- Are we using good cyber hygiene?

When deciding how to move forward with strengthening a cybersecurity program, manufacturers should keep in mind the need to safeguard devices against malicious and non-malicious attacks. Vulnerable devices can become infected by malware that cannot discern the difference between a personal computer and a pacemaker. That example is not farfetched—J.M. Porup recently reported for *Slate* that malware designed to steal credit card information infected and disabled vulnerable fetal heart monitors.

The choice of a lawyer is an important decision and should not be based solely upon advertisements.

ABOUT SHOOK

Shook, Hardy & Bacon is widely recognized as a premier litigation firm in the United States and abroad. For more than a century, the firm has defended clients in some of the most significant national and international product liability and mass tort litigations.

Leading pharmaceutical and medical device companies rely on Shook to advance their business interests in the courtroom and beyond. More than 100 Shook attorneys are involved in the defense of product liability, commercial, intellectual property, and other litigation specifically for pharmaceutical and medical device manufacturers.

We also guide clients through an ever-changing patchwork of data security and data privacy laws and regulations, and helps its clients manage litigation and other risks associated with maintaining and using electronic information.

ACC Association of Corporate Counsel
VALUE CHAMPION
2012 | 2013 | 2015