ReedSmith

Client Alert

Life Sciences Health Industry

Cybersecurity for Medical Devices: A Risk Mitigation Checklist for In-House Counsel

If you have questions or would like additional information on the material covered in this Alert, please contact one of the authors:

Steven J. Boranian
Partner, San Francisco
+1 415 659 5980
sboranian@reedsmith.com

Colleen T. Davies
Partner, San Francisco
+1 415 659 4769
cdavies@reedsmith.com

Barry J. Coyne
Partner, Pittsburgh
+1 412 288 7210
bcoyne@reedsmith.com

…or the Reed Smith lawyer with whom you regularly work.

Just this summer, a cybersecurity firm issued a report widely cited in the media detailing cases where unnamed hospitals were allegedly hit by data breaches after medical devices (identified only generically as a blood gas analyzer, a picture archive and communications system (PACS), and an X-ray system) became infected with malware or backdoors that allowed hackers to move within the health care network. (*See*, e.g., http://www.computerworld.com/article/2932371/cybercrime-hacking/medjack-hackers-hijacking-medical-devices-to-create-backdoors-in-hospital-networks.html).

In addition, the FDA issued a Safety Alert in May of 2015 about cybersecurity vulnerabilities in an infusion pump. While this Alert was preventative and not the result of any actual breach, it described a common cybersecurity risk for medical devices:

> Many medical devices contain configurable embedded computer systems that can be vulnerable to cybersecurity breaches. In addition, as medical devices are increasingly interconnected, via the Internet, hospital networks, other medical device, and smartphones, there is an increased risk of cybersecurity breaches, which could affect how a medical device company operates. http://www.fda.gov/Safety/MedWatch/SafetyInformation/SafetyAlertsforHumanMedicalProducts/ucm456832.htm

Notably, it is not usually an option to simply "disconnect" devices or otherwise disable their remote connectivity, as information transmitted remotely by medical devices to health care professionals can and does protect patient health. Additionally, medical device manufacturers do not control the hospital networks or health care organizations where their devices are used. Nor do they communicate directly with patients who use the devices.

Recognizing these challenges, the FDA has issued several guidance documents concerning cybersecurity for medical devices, including:

- Content of Premarket Submissions for Management of Cybersecurity in Medical Devices; Guidance for Industry and Food and Drug Administration Staff; Availability (*See* https://www.federalregister.gov/articles/2014/10/02/2014-23457/content-of-premarket-submissions-for-management-of-cybersecurity-in-medical-devices-guidance-for)
- Cybersecurity for Medical Devices and Hospital Networks: FDA Safety Communication (*See* http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm)
- Information for Healthcare Organizations about FDA's "Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-The-Shelf (OTS) Software" (*See* http://www.fda.gov/RegulatoryInformation/Guidances/ucm070634.htm)
- Guidance for Industry – Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software (*See* http://www.fda.gov/RegulatoryInformation/Guidances/ucm077812.htm)

Reed Smith's IP, Information & Innovation and Life Sciences Health Industry Groups have therefore joined up to create a Task Force of specialty legal practices to guide medical device and other medical application companies through a risk mitigation assessment process so as to (1) prevent cyber breaches in the first instance, and (2) reduce legal risks should one occur.

Below is a starting place: a Risk Mitigation Checklist for in-house counsel of medical devices to consider.

Given the complexity of the issues, this Checklist is by necessity not exhaustive. That said, it does span a host of issues that any medical device company will face by reason of having embedded computer systems and/or Internet connections that are vulnerable to securities breaches.

Reed Smith's Task Force will explore many of the risk issues covered in this checklist in more detail in future blog postings. In the meantime, we hope that this is a helpful launching pad for internal company risk assessments of how to prevent hacking and other security breaches.

Risk Mitigation Checklist The following checklist outlines issues medical device companies should assess when conducting a cybersecurity risk assessment in order to (1) prevent cyber breaches in the first instance, or (2) help defend against security breach claims, regulatory violation allegations, or injury or damage lawsuits. Where possible, such a risk assessment should be conducted under the protection of applicable legal privileges in anticipation of litigation, and in order

to mitigate a variety of legal risks, including exposure to regulatory action or to personal or financial injury claims.

Are cybersecurity protocols and practices in place at the company? It is absolutely essential that a written security policy be in place so as to ensure that:

- The analysis of potential cybersecurity threats is an ongoing process that is routinely updated.
- Company policies, procedures and controls are in place for preventing unauthorized access or modification to the company's devices and systems – as well as to any connected hospital or third-party networks.
- Technical security controls are in place, such as firewalls, passwords, multiple authentication methods, and anti-virus software for devices, computers and networks.
- Policies and procedures exist to control and limit employee access to the company's information technologies and systems.

Does the company conduct an ongoing assessment of cybersecurity risks? In the event of a breach, the company will need to establish its ongoing vigilance and risk assessment, including evidence showing:

- The company is assessing, and when necessary, taking corrective action responsive to cybersecurity vulnerabilities (per obligations under 21 CFR 820.100 (http://www.gpo.gov/fdsys/granule/CFR-2002-title21-vol8/CFR-2002-title21-vol8-sec820-100).
- Security controls are in place and are regularly updated (this will depend upon factors such as the type of device, probability and type of risks to patients).
- Authorized device access is strictly limited to trusted users only.
- Desktop and system audits are conducted.
- The company monitors, logs, and reports all intrusions or attempted intrusions.

Does the company have a training program in place to ensure that cybersecurity protocols are known and followed? If security claims should later arise, claimants will seek to establish that company employees either failed to follow or were unaware of existing security policies. To mitigate potential claims, in-house counsel should assess the following:

- Are training and compliance programs in place?
- Is training regularly updated to address new threats?
- Is attendance mandated for relevant groups of employees and is attendance tracked?

Has the Legal Department reviewed all indemnity and warranty protections with suppliers and component part manufacturers? One major way of mitigating liability risks for cyber breaches is to assess on the front end contractual liability in the event of breach. The Legal Department's action list should include the following:

- A review of supplier agreements to determine if indemnity and warranty provisions include protection in the event of cybersecurity breaches – and action to update such agreements if they are not.
- For third-party business arrangements, a review of that company's cybersecurity policies, practices and vulnerabilities – and action to request changes if prudent.
- An analysis of what gaps exist in indemnity protections – including whether the company has the right to control the defense, select counsel, and make settlement decisions in the event lawsuits or claims arise.

Are regulatory compliance and risk-hazard assessments conducted at the design, testing and manufacturing stages of product development? In-house counsel should work with the IT department and other relevant groups to ensure that a proactive design-hazard analysis includes:

- Attention to the issues identified by the FDA in its issuance of *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices* on October 2, 2014 (which sets forth the information related to the cybersecurity that manufacturers should provide in their premarket submission for their medical device). (*See* https://www.federalregister.gov/articles/2014/10/02/2014-23457/content-of-premarket-submissions-for-management-of-cybersecurity-in-medical-devices-guidance-for)
- Preparing hazard analysis, mitigations, and design considerations pertaining to intentional and unintentional cybersecurity risks associated with the device, including:
  - A list all cybersecurity risks that were considered in the design of the device
  - Justification for all cybersecurity controls that were established for the device
- Efforts by the company to implement features in its devices that allow for security compromises to be detected, recognized, logged, timed, and acted upon during normal use.
- Implementing device features that protect critical functionality, even when the device's cybersecurity has been compromised.

Does the company have a Corrective Action Readiness Plan in place for a potential cybersecurity breach – as well as an established Communications Plan? The company needs to be ready to respond both internally and externally in the event of a cybersecurity breach. Given that medical device companies do not control the hospital networks or health care organizations where the devices are, there are shared responsibilities:

- Device manufacturers should consider having an external communications plan in place for disclosure of any breach, and a description of the company's mitigation efforts. Such a plan should address any specific questions and concerns that might exist for relevant audiences (e.g., regulatory agencies, employees, media, investors).
- While not under the control of the device manufacturer, physicians and hospitals will need to be ready to provide information to the end user concerning appropriate actions to take upon detection of a cybersecurity breach. This should include methods for retaining operability or recovering information.

Has there been an insurance coverage assessment to ensure coverage exists in case of breach? The company should review its insurance portfolio to determine which policies provide coverage in the event of a data breach or privacy event.

- While cyber liability insurance is an important part of a company's portfolio, other policies may well provide coverage and therefore should be reviewed and analyzed as well.
- A risk analysis should be conducted on the front end since the terms and conditions of policies can vary – and can and should be negotiated before any event occurs.
- There should be an advance understanding of what steps are needed under relevant insurance policies in the event of a data breach or privacy event. Timely notice is critical, as is an understanding of who gets to select the attorneys and third-party service providers that will help investigate and remediate the event.
- A privileged assessment should take place of what documentation will be needed to support a claim for insurance loss.

Has an analysis been conducted of disclosure duties to patients, doctors and health care networks? As the FDA has recognized, medical device security is a shared responsibility between health care facilities, patients, providers, and manufacturers of medical devices. This requires analysis of what information should be shared with patients, doctors and health care networks so that they may assist in maintaining cybersecurity:

- Appropriate warnings and procedures concerning cybersecurity are included in instructions for use.
- Cybersecurity protocols and practices are included in training patients, doctors and health care networks.
- Placement and use of devices is available so that doctors and health care networks using the devices can be contacted for security updates, or in the event of security breaches.

Has the Legal Department analyzed what potential financial or other disclosure duties might exist (e.g., to shareholders, board of directors, potential buyers, etc.) if a breach occurs? The severe impact cybersecurity attacks can have on the company may trigger mandatory disclosures to company stakeholders and the public. In-house counsel should consider whether information concerning cybersecurity and cyber-incidents rises to the level of a reportable event.

Does the company have a plan and procedure for reporting intrusions or breaches to the FDA or other governmental authorities?

- In the event of a security breach, manufacturers must comply with the Medical Device Reporting (MDR) regulations. (http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/PostmarketRequirements/ReportingAdverseEvents/ucm2005737.htm)
- FDA has encouraged reporting if a cybersecurity event has impacted the performance of a medical device or has impacted a hospital network system, by filing a voluntary report through MedWatch, the FDA Safety Information and Adverse Event Reporting program. (http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm)
- Consider whether a report should be filed with Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT). (http://www.dhs.gov/report-cyber-risks)

Does the company have personnel, procedures and policies in place for addressing customer and end-user concerns? The FDA recommends that purchasers and users of medical devices that may be subject to cybersecurity vulnerability contact manufacturers with their concerns. As such, the company should be prepared to provide advice and recommendations to customers and end users.