crowell moring

# CLIENT ALERT

## FDA Publishes Cyber Guidance for Medical Devices

**Oct.07.2014**

**On October 2, 2014, the FDA released a set of guidelines designed to improve the cybersecurity of medical devices and to combat increasing vulnerability to cyber-attacks. Compliance with the guidelines, although not mandatory, is strongly recommended to protect not only patients, but also manufacturers, facilities, and providers. In drafting the guidelines, the FDA was careful to consider the particular sensitivities involved in the regulation of instruments designed for health care. Overly strict regulations may run the risk of inhibiting a device's functional capabilities – a distinct concern in the case of devices intended for emergency response. Conversely, if regulations are not strict enough, there is an increased risk of potential cyber incidents that could result in patient harm such as illness, injury, or even death.**

**The FDA suggests that manufacturers address cybersecurity issues during the design and development of medical devices. The general guidelines propose that manufacturers identify any assets, threats, and vulnerabilities of a new medical device; assess the likelihood of a security incident and its potential impact on device functionality and end users; determine the level of risk and mitigation strategies; and assess residual risk and risk acceptance. Notably, however, there is no requirement that manufacturers revisit existing devices to ensure adequate security measures are in place. Also notable is that application of the guidelines is not limited to devices that have the ability to connect to another device or to portable media (though the guidelines call for additional cybersecurity measures with respect to such connected devices).**

**The recommendations next focus on cybersecurity functions, which mirror those laid out in the NIST Cybersecurity Framework - *i.e.*, the process to Identify, Protect, Detect, Respond, and Recover. Here, the identification and protection steps require a case-by-case analysis of the specific threats and vulnerabilities of each device. For example, devices that carry higher risk – such as those that contain sensitive information or that could significantly harm a patient if tampering occurred – will likely require increased security controls. There is, however, a practical need to balance security controls with the ability to have complete access to a fully functioning medical device when necessary.**

**The FDA also provides some real-world examples of appropriate protection measures. These include, but are not limited to, stricter user authentication; stronger passwords; physical locks when available; automated timing systems for logging users**

**Recent Happenings in APRM**
**October 2014**

- When Internet Connectivity Features Fail – is the Product Unsafe, or Just Not "Smart"?
- The European Commission Issues a "Myth-Busting" Factsheet to Address the Concerns That Have Emerged After the EU Court of Justice's Ruling On Search Engines and the "Right to Be Forgotten"
- Think of the Children: Guidelines for Advertising Food and Alcohol
- Proposition 65 – Warning Regulation Update
- Why You Should Comment on the CPSC Certificate of Compliance Filings at Entry
- California Enacts Tough New Privacy Protections
- FDA Publishes Cyber Guidance for Medical Devices
- To Label Or Not To Label? Companies May Have No Choice

**out of inactive sessions; and secure data transfer using encryption when possible. Manufacturers are also instructed to implement features within devices that will detect a security breach while maintaining functionality in the event of device compromise, and to have methods in place for retention and recovery of compromised information.**

**Finally, the FDA provides guidelines for documenting the manufacturers' efforts in premarket submissions. Identification of risks should be outlined in detail, and protection mechanisms justified. The FDA would also like to see the link between each cybersecurity control and the corresponding risk it is intended to combat. Submissions should further document the device's update schedule and include specific instructions for the use and implementation of the cybersecurity controls identified.**

**The FDA's cybersecurity guidelines for medical devices reflect growing scrutiny by government agencies regarding collection and storage of sensitive information. The unique challenges in sufficiently safeguarding hypersensitive medical information connected to medical devices require balancing adequate security controls and the need for medical instruments to operate as intended despite any incident that may arise during operation of the device. The guidelines provide a framework for enabling manufacturers to conduct their own risk assessments and weigh security risks against other considerations in the development of medical devices.**

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

**Evan D. Wolff**
Partner – Washington, D.C.
Phone: +1 202.624.2615
Email: ewolff@crowell.com

**John Fuson**
Partner – Washington, D.C.
Phone: +1 202.624.2910
Email: jfuson@crowell.com