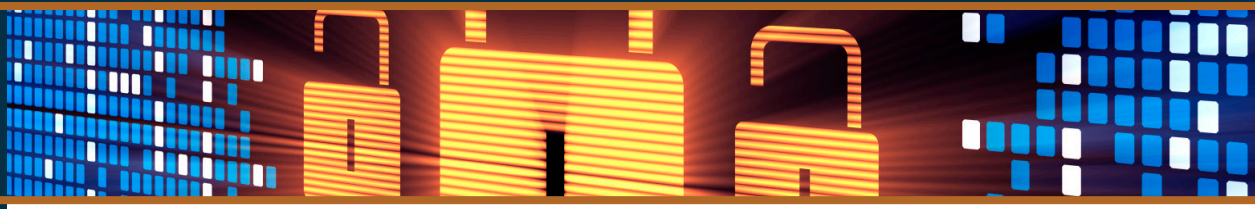
SHIPMAN & GOODWIN® LLP
COUNSELORS AT LAW

LIFE SCIENCES AND MEDICAL PRODUCTS ALERT

June 25, 2013



FDA Releases Draft Cybersecurity Guidance for Medical Devices:

Provides Recommendations to Both Manufacturers and Health Care Facilities

Questions?
If you have any questions about this alert, please contact:

Joan W. Feldman
(860) 251-5104
jfeldman@goodwin.com

David M. Mack
(860) 251-5058
dmack@goodwin.com

William J. Roberts
(860) 251-5051
wroberts@goodwin.com

www.shipmangoodwin.com

The FDA recently released draft guidance for medical device manufacturers[1] and a safety communication for manufacturers and health care facilities[2] regarding cybersecurity issues with the manufacture, approval and use of medical devices. Specifically, the FDA provides recommendations regarding how manufacturers should address cybersecurity in the design of medical devices and in premarket submissions[3], and how health care facilities should ensure network security. While the draft guidance and safety communication are not legally binding and are subject to change, they provide important insight into how the FDA will be reviewing premarket submissions and the attention it will pay to cybersecurity matters.

1. Manufacturing Recommendations.

When developing medical devices involving the use, transmission or storage of data (such as patient information or results), the FDA encourages manufacturers to develop and implement security controls in the device to assure the confidentiality, integrity and availability of the data. The FDA also encourages manufacturers to conduct and document the following components of a "cybersecurity risk analysis and management plan":

- Identification of assets, threats and vulnerabilities;
- Assessment of the threats and vulnerabilities on device functionality;
- Assessment of the likelihood of a threat and of a vulnerability being exploited;
- Determination of risk levels and suitable mitigation strategies; and
- Residual risk assessment and risk acceptance criteria.

---

1 A copy of the draft guidance is available at: http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf

2 A copy of the safety communication is available at: http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm

3 The guidance documents apply to the following submissions: (i) premarket notification (510(k)) including traditional, special, and abbreviated submissions; (ii) *de novo* petitions; (iii) premarket approval applications; (iv) product development protocols; and (v) humanitarian device exemptions.

When deemed necessary or advisable by the risk analysis, manufacturers should consider appropriate security controls such as access restrictions, failsafe and recovery features, strong passwords, and multi-layer and multi-factor authentication. The FDA acknowledges that the security controls adopted, and the extent of those controls, will depend on the specific medical device and its use, environment, and relationship to patient information. On the whole, the FDA considers devices capable of connecting to another device, to the Internet or a closed network, or to portable media (such as a USB drive) as more vulnerable to cybersecurity threats than other devices.

2. Premarket Submission Recommendations.

The FDA recommends that manufacturers provide in their premarket submissions justification for the security controls chosen and the following information related to the cybersecurity of the device:

- Hazard analysis, mitigations, and design considerations pertaining to cybersecurity risks;
- A traceability matrix that links cybersecurity controls to the cybersecurity risks considered;
- A plan for providing validated updates and patches to medical device software;
- Appropriate documentation to demonstrate that the device will be provided to purchasers and users free of malware; and
- Device instructions related to recommended anti-virus software and/or firewall use.

3. Recommendations for Health Care Facilities.

In light of the increased number and variety of medical devices that may connect to health care facility networks, and the risks involved with such connectivity, the FDA recommends that health care facilities evaluate network security with medical devices in mind. Despite FDA efforts to improve the cybersecurity controls and lessen the vulnerabilities of medical devices, health care facilities should be aware that some devices might lack sufficient safeguards and be a conduit for viruses, malware, “worms” and other network threats. Specifically, the FDA encourages health care facilities to:

- Restrict unauthorized access to their networks and networked medical devices;
- Ensure that antivirus software and firewalls are up-to-date;
- Monitor network activity for unauthorized use;
- Protect individual network components through routine and periodic evaluation;

- Contact the device manufacturer upon discovery of a cybersecurity concern; and
- Develop strategies to maintain critical functionality during adverse conditions.

While health care facilities are likely already addressing many of these recommendations through periodic HIPAA risk assessments and IT security programs, health care facilities should incorporate these standards into their assessments to ensure that medical devices connecting to and utilizing their networks are properly secured.

4. Our Perspective.

Manufacturers should note that the FDA has been paying increased attention to cybersecurity and data privacy concerns with respect to medical devices with a particular emphasis on mobile medical devices (such as smartphone apps). As such, manufacturers will need to evaluate how to address these issues when developing their products and preparing their premarket submissions.

Health care facilities are encouraged to monitor FDA medical device recommendations and the proliferation of network-connected devices and assess how such developments will affect their operations and network security. Device connectivity to facility networks should be added to facility risk assessment programs and addressed during any applicable contract negotiations, particularly with respect to the use of facility network infrastructure and the use and transfer of patient information. Facilities should also be aware that FDA recommendations may create certain industry standards of care that may impact HIPAA security requirements.

If you have any further questions about this alert or medical device or hospital network security in general, please contact any member of Shipman & Goodwin's **Health Law Practice Group** or **Life Sciences and Medical Products Team.**

One Constitution Plaza
Hartford, CT 06103-1919
860-251-5000

300 Atlantic Street
Stamford, CT 06901-3522
203-324-8100

1133 Connecticut Avenue NW
Washington, DC 20036-4305
202-469-7750

289 Greenwich Avenue
Greenwich, CT 06830-6595
203-869-5600

12 Porter Street
Lakeville, CT 06039-1809
860-435-2539

www.shipmangoodwin.com

SHIPMAN & GOODWIN® LLP