HALL RENDER
KILLIAN HEATH & LYMAN

HEALTH LAW NEWS

OCTOBER 09, 2014

FDA ISSUES GUIDANCE FOR CYBERSECURITY IN MEDICAL DEVICES

EXECUTIVE SUMMARY

While the notion of malicious hacking of a medical device has been a recent topic in fictional television shows, it became a public reality in October 2013 when former Vice President Dick Cheney revealed that his cardiologist modified Cheney's heart defibrillator to disable a wireless feature and prevent hacking of the device. To date, providers have reported that medical devices such as X-ray and CT scanners and devices in cardiac catheterization labs that connect to a provider's information technology infrastructure have been hacked, but devices that operate independently of information technology such as infusion pumps, fetal monitors and implantable pacemakers have also been viewed as vulnerable.

On October 2, 2014, the Food and Drug Administration ("FDA") released a guidance document concerning the content of premarket submissions for management of cybersecurity in medical devices (the "Guidance"). The FDA found that the need for effective cybersecurity has become more important due to the surge of wireless, Internet- and network-connected devices and the frequent electronic exchange of medical device-related health information. The Guidance identified cybersecurity issues that manufacturers should consider when preparing premarket submissions for medical devices. The full text of the Guidance is available here. This Guidance was preceded by the FDA's June 13, 2013 safety communication regarding cybersecurity concerns for medical devices, including vulnerability to threats of hacking and malware.

FDA GUIDANCE

The Guidance recommends that manufacturers address cybersecurity during the design and development of medical devices, including the establishment of a cybersecurity vulnerability and management approach as part of their required software validation and risk analysis under 21 C.F.R. 820.30(g). The FDA provided the following framework to help guide manufacturers in their cybersecurity activities:

- **Identify**: Determine whether the medical device is capable of connecting to another device, the Internet or other network or to portable media.
- **Protect**: Include appropriate safeguards in medical devices while balancing the need for cybersecurity with the usability of the device, including in what context the medical device is used.
- **Detect**: Implement features that allow for security compromises to be detected, recognized, logged, timed and acted upon during normal use.
- **Respond**: Provide information to the end user concerning actions to take upon detection of a cybersecurity event and implement features that protect critical functionality after the event.
- **Recover**: Provide methods for retention and recovery of device configuration by an authenticated privileged user.

The FDA also provided the following recommendations for the type of cybersecurity documentation a medical device manufacturer should include in a premarket submission:

- Hazard analysis, mitigations and design considerations pertaining to intentional and unintentional cybersecurity risks associated with the device;
- Traceability matrix that links actual cybersecurity controls to considered cybersecurity risks;
- Summary of a plan for software updates as needed throughout the life of the device;
- Summary of controls to ensure the device software will maintain integrity from the point of origin to the point where the device leaves manufacturer control; and
- Device instructions for use and product specifications related to recommended cybersecurity controls appropriate for the intended use

environment.

The Guidance applies to the following premarket submissions for medical devices that contain software or programmable logic: 510(k) premarket notifications; *De novo* submissions; premarket approval applications; product development protocols; and humanitarian device exemption submissions.

The FDA is hosting a public workshop on this subject October 21-22, 2014, in an effort to collaborate with medical device manufacturers, health care facilities and state and federal governments to identify and address cybersecurity challenges facing the industry. Stakeholders should pay close attention to the outcome of the workshop to better address potential vulnerabilities prior to premarket submission.

RISKS AND PRACTICAL TAKEAWAYS

Vulnerabilities in cybersecurity present serious risks that could impact patient care. Exploitation of vulnerabilities may result in medical device malfunction, disruption of health care services, compromised integrity of electronic health records or harm to a patient. The FDA stated that the risks associated with these vulnerabilities only increase as the interconnectivity of devices expands. Some key considerations with respect to cybersecurity of medical devices and the FDA's Guidance include:

- Providers and medical device manufacturers developing new technology should strongly consider following the recommendations provided in the Guidance when developing new products prior to premarket submissions.
- Medical device manufacturers should evaluate their existing medical devices for cybersecurity risk to ascertain whether adjustments need to be made to prevent unauthorized access in accordance with the Guidance. Breached cybersecurity in the medical device may give rise to a products liability claim in the event a patient is harmed.
- Providers should review supply chain contracts to confirm inclusion of or to negotiate in indemnification obligations for medical device manufacturers for products liability claims and breaches of cybersecurity of the medical device.
- Providers should request information for medical device manufacturers on what steps have been taken to mitigate the risk of cybersecurity breaches for medical devices being purchased.
- Providers should educate their employees and patients of the cybersecurity risks associated with applicable medical devices.

If you have any questions or would like additional information about this topic, please contact:

- Jeffrey W. Short at (317) 977-1413 or jshort@hallrender.com;
- Jennifer P. Viegas at (317) 977-1485 or jviegas@hallrender.com;
- GinaMarie F. Geheb at (248) 457-7823 or ggeheb@hallrender.com; or
- Your regular Hall Render attorney.

Special thanks to Matthew W. Decker for his assistance with the preparation of this Health Law News article.

Please visit the Hall Render Blog at hallrender.com/resources/blog for more information on topics related to health care law.