FDA RELEASES FINAL POST-MARKET GUIDANCE ON MEDICAL DEVICE CYBERSECURITY

On December 27, 2016, the Food and Drug Administration ("FDA") issued final guidance (the "Post-Market Guidance") outlining steps that medical device manufacturers and health care systems should take to monitor, identify, understand and address cybersecurity risks once medical devices and mobile medical devices have entered the marketplace. The Post-Market Guidance follows October 2014 FDA guidance addressing premarket cybersecurity issues for medical devices that are still in development. Taken together, the pre-market and Post-Market Guidance recommends robust cybersecurity controls during the medical device development process, continuous threat-monitoring throughout a product lifecycle by all stakeholders and rapid responses to threats.

BACKGROUND OF CYBERSECURITY

Although software and hardware design controls can be included in medical devices to help reduce cyber risk, the evolving nature of cyber threats may require some medical device manufacturers and health care systems to invest more time and resources towards thwarting such risks in existing products. Additionally, the FDA has indicated that post-market medical device improvements, updates and new features may increase the vulnerability of such medical devices. The FDA has previously encouraged medical device manufacturers and health care systems to apply the core rules of National Institute of Standards and Technology ("NIST") as a part of a comprehensive cybersecurity risk management program to improve cybersecurity infrastructure and mitigate risk. Recommendations are intended to address the potential risks associated with a cyber breach that could affect a medical device's performance and functionality - and ultimately impact patient health.

FDA RECOMMENDATIONS

The Post-Market Guidance, entitled *Postmarket Management of Cybersecurity in Medical Devices,* provides a proactive and risk-based approach that medical device manufacturers and health care systems can utilize to maintain medical device security. The Post-Market Guidance outlines what the FDA considers "good cyber hygiene" practices and reinforces the FDA's earlier public positions on medical device security (including the FDA's draft guidance on the same topic posted on January 22, 2016). Suzanne B. Schwartz, the FDA's associate director for science and strategic partnerships, stated in a concurrent blog post that the FDA believes that the Post-Market Guidance will increase patient safety, improve medical device effectiveness and mitigate the risks associated with cybersecurity threats.[1] To answer questions regarding the guidance, the FDA will hold a January 12, 2017 webinar that can be accessed here.

The Post-Market Guidance notes that cybersecurity risks are especially prevalent in the "Internet of Things" ("IoT") product category (ie., products that are networked together) in part because of broad adoption of IoT products throughout hospitals, clinics, workplaces and homes and in part due to increased cyber activity targeting IoT products. Recent headlines have shown that hospital networks and IoT medical devices frequently experience intrusion and attack attempts, which may pose a threat to patient safety, protected health information ("PHI") and other confidential information.[2] As it relates to personal wearable devices such as Fitbits and iWatches, previous FDA guidance has suggested that the FDA will not vigorously regulate personal wearable devices in the same way as it does traditional medical devices as long as such personal wearable devices are not deemed harmful and generally encourage healthy habits. However, wearable device manufacturers and trade associations have repeatedly asked the FDA to define exactly where the regulated medical device threshold is, and it is unclear whether the FDA's increased emphasis on medical device security (including this Post-Market Guidance) is due in part because of the rapid consumer uptake of personal wearable devices.

NOTIFICATION AND FDA REPORTING REQUIREMENTS

The Post-Marketing Guidance emphasizes the need for proactive communication regarding cyber vulnerabilities among stakeholders to help mitigate the impact of systemic risks. The FDA now recommends that medical device manufacturers participate in an Information Sharing Analysis Organization ("ISAO") where public and private entities can share cybersecurity information.

The Post-Market Guidance addresses when updates to address cybersecurity risks must be reported to the FDA as well as a protocol for assessing risk(s) posed by the medical device that may result in patient harm. More specifically, although routine updates or patches to

address cyber threats would not require advance notification or reporting to the FDA, medical device manufactures must notify the FDA for vulnerabilities for uncontrolled risks that could impact clinical performance or present a reasonable probability of serious adverse health consequences or patient death.[3] The Post-Market Guidance also states circumstances where the FDA does not intend to enforce reporting requirements under 21 CFP part 806, and participation in an ISAO is one of the factors to qualify for such exemption.

Finally, notably absent from the Post-Market Guidance were plans for the how the FDA would enforce these rules.

PRACTICAL TAKEAWAYS

In light of the Post-Market Guidance, medical device manufacturers, health care systems and providers should implement structured and comprehensive programs to manage cybersecurity throughout product lifestyle stages, including:

- Monitoring and detecting cybersecurity vulnerabilities across all medical devices, especially those medical devices and personal wearable devices with network capabilities;
- Engaging stakeholders across the cybersecurity community to obtain information about potential and current vulnerabilities;
- Developing plans to identify, assess and address vulnerabilities that pose concerns to functionality and patient safety, including deploying mitigations (patches, updates, etc.) to address vulnerabilities before they can be exploited and cause significant harm; and
- Providing practical guidance to personnel and patients using medical devices in clinical and non-clinical settings.

Entities that provide medical devices to patients, including hospitals and medical providers, should pay special attention to this Post-Market Guidance.

If you have any questions, or would like additional information about this topic, please contact Tony Caldwell at (317) 977-1469 or acaldwell@hallrender.com or your regular Hall Render attorney.

[1] http://blogs.fda.gov/fdavoice/index.php/2016/12/managing-medical-device-cybersecurity-in-the-postmarket-at-the-crossroads-of-cyber-safety-and-advancing-technology/

[2] For a helpful summary, please see *A Brief Chronology of Medical Device Security,* A. J. Burns, M. Eric Johnson, and Peter Honeyman, Communications of the ACM, Vol. 59 No. 10, Pages 66-72.

[3] Although 21 CFR part 806 requires device manufacturers to promptly report certain actions concerning medical device corrections and/or removals, this guidance clarifies that "cybersecurity routine updates and patches" are excluded from reporting under a device enhancement exception. Click here for more information on this topic.

Please visit the Hall Render Blog at http://blogs.hallrender.com/ or click here to sign up to receive Hall Render alerts on topics related to health care law.