DEPARTMENT OF HOMELAND SECURITY AND FDA COLLABORATE TO ADDRESS MEDICAL DEVICE CYBERSECURITY

On October 15, 2018, the National Protection and Programs Directorate ("NPPD") of the U.S. Department of Homeland Security ("DHS") and the U.S. Food and Drug Administration ("FDA") entered into a Memorandum of Agreement ("MOA") that formalizes a long-standing relationship between the agencies and implements a new framework for increased collaboration, information-sharing and coordination that addresses cybersecurity in medical devices.[1] The FDA and DHS hope that by strengthening their partnership they can stay "a step ahead of constantly evolving medical device cybersecurity vulnerabilities and assist the health care sector in being well positioned to proactively respond when cyber vulnerabilities are identified."[2] Under the MOA, DHS will continue to serve as the central medical device vulnerability coordination center and will consult with FDA for its expertise on medical devices. The MOA can be found here.

BACKGROUND

The FDA's Center for Devices and Radiological Health ("CDRH") ensures that patients and providers have access to safe and effective medical devices. Medical devices are increasingly becoming interconnected and interoperable, making them vulnerable to cybersecurity risks that could affect device performance and patient safety. All types of medical devices, ranging from implantable cardiac pacemakers and defibrillators that have wireless capability to infusion pumps, CT scanners and MRIs, communicate with other networked devices. This ability to communicate creates cyber risk. Hackers may either seek to interfere in the transmission, change the data or simply disrupt the network and prevent the data from being transmitted at all. It is easy to envision the risk that a patient might face when incorrect, or no, information is transmitted due to such a system disruption. CDRH monitors, identifies and addresses cybersecurity vulnerabilities in medical devices to manage these types of risk.

DHS is the lead agency for the protection of critical infrastructure and cybersecurity, and a core component of the DHS's mission is to prevent terrorism and enhance security. DHS's NPPD works to secure cyberspace, prevent or minimize disruptions to vital information infrastructure and protect the public as well as government services.

KEY PROVISIONS OF THE MOA

Here are some of the key provisions in the MOA:

a. NPPD of DHS and FDA will collaborate to enhance awareness of medical device cybersecurity vulnerabilities.

b. The National Cybersecurity and Communications Integration Center ("NCCIC") of the NPPD of DHS will coordinate and facilitate information sharing between medical device manufacturers, researchers and the FDA's CDRH particularly with respect to cybersecurity vulnerabilities in medical devices. Exchanged information may contain certain private, confidential or protected information, which will be secured from unauthorized use and further disclosure subject to applicable laws, regulations and appropriate consents.

c. If there is a need, NPPD can assist FDA as an independent third party in the evaluation and assessment of the impact of medical device vulnerabilities.

d. NPPD and FDA will participate in regular, ad hoc and emergency coordination calls to enhance mutual awareness of cybersecurity vulnerabilities and threats.

e. Within 90 days of full execution of the MOA, NCCIC and CDRH will develop a standard operating procedure for information sharing and exchange.

f. NPPD will:
   a. Coordinate with FDA on the content of alerts and advisories related to medical device cybersecurity to be published by DHS; and
   b. Confer with entities providing sensitive information regarding medical devices and after clearance, notify FDA of device vulnerabilities.

g. FDA will:
   a. Provide NPPD with draft public releases for review to facilitate federal agency coordination of messaging;
   b. Make assessments regarding the risk to health and the risk of patient harm when the potential impact of a medical device cybersecurity vulnerability is disputed; and
   c. Obtain NPPD's independent third-party technical assistance to analyze and test medical systems.

PRACTICAL TAKEAWAYS

This collaboration between the FDA and DHS further highlights how seriously the FDA is taking security of medical devices. Recently, the FDA has stepped up enforcement actions against medical device manufacturers and health care providers related to device security. And, on October 18, the FDA released draft guidance to the medical device and health care industry regarding cybersecurity device design, labeling and documentation that the FDA recommends be included in premarket submissions for devices with cybersecurity risk.[3] Because medical device cybersecurity is a shared responsibility for all stakeholders, health care providers and device manufacturers should work together to evaluate cybersecurity threats and vulnerability to better protect patient safety and privacy. FDA's recent actions and guidance emphasize that information sharing regarding vulnerabilities and indicators of compromise is one important way to minimize cybersecurity risks and further protect patient data.

Our privacy and cybersecurity attorneys can assist you in leveraging cybersecurity activities to improve patient safety and quality, support participation in information sharing activities that help improve security and ensure patient confidentiality.

For further information, please contact:

- Adele Merenstein at (317) 752-4427 or amerenstein@hallrender.com;
- Melissa Markey at (248) 740-7505 or mmarkey@hallrender.com;
- Mark Garsombke at (414) 721-0907 or mgarsombke@hallrender.com; or
- Your regular Hall Render attorney.

[1] FDA News Release: *FDA and DHS increase coordination of responses to medical device cybersecurity threats under new partnership; a part of the two agencies' broader effort to protect patient safety* (Oct. , 2018) available at: https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm623574.htm.

[2] FDA Commissioner Scott Gottlieb, M.D. from FDA News Release.

[3] FDA, *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices - Draft Guidance for Industry and Food and Drug Administration Staff* (October 18, 2018).