SQUIRE PATTON BOGGS

# Digital Health Update: Recent Food and Drug Administration Cyber Initiatives

The Food and Drug Administration (FDA) has greatly increased its activity around cybersecurity initiatives and medical devices. As we approach the end of the year, this is a great opportunity to review recent developments.

## FDA Medical Device Cybersecurity Guidance

On October 18, 2018, the FDA published draft guidance, "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices." When finalized, this draft will replace prior guidance from 2014. The document outlines recommendations for device design, data confidentiality, labeling conventions and cybersecurity documentation. Key requirements include:

- Risk-based categorization of devices into two tiers (based primarily upon device connectivity and risk of cybersecurity incidents)
- Preparation of a cybersecurity bill of materials listing device components that could be vulnerable to cybersecurity incidents
- Authentication before software or firmware updates
- Application of the NIST Cybersecurity Framework

The public comment period will end on March 18, 2019, and there will be a workshop open to the public on January 29-30, 2019. Industry professionals should take this opportunity to determine the effects this guidance could have on device approval in the future and consider commenting.

## Partnership With Department of Homeland Security

The FDA and the Department of Homeland Security (DHS) announced on October 16, 2018, that the parties had entered into a memorandum of agreement (MOA) for Medical Device Cybersecurity Collaboration. The FDA's press release described the agreement between FDA's Center for Devices and Radiological Health (CDRH) and DHS' National Protection and Programs Directorate (NPPD) as "meant to encourage even greater coordination and information sharing about potential or confirmed medical device cybersecurity vulnerabilities and threats." Under the agreement, NPPD shall serve as the central medical device vulnerability coordination center, provide independent third-party assistance to the FDA for technical assessments and share information. The FDA shall coordinate regular communications with NPPD regarding cybersecurity vulnerabilities and threats, make cybersecurity vulnerability assessments and share information.

## Cybersecurity Playbook: Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook

On October 1, 2018, the MITRE Corporation released the Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook, developed in collaboration with the FDA and industry stakeholders. MITRE is a nonprofit that operates federally funded research and development centers and has assisted the FDA with growing its cybersecurity program at CDRH. The Playbook responds to concerns by industry stakeholders, including medical device manufacturers (MDMs) and healthcare delivery organizations (HDOs), that they needed additional information and resources on how to respond to cybersecurity incidents such as the WannaCry event. It includes a customizable framework with recommendations that HDOs can use to "leverage as a part of their emergency response plans" to minimize patient care disruptions and harm that could occur from a medical device cybersecurity incident. Topics covered include items such as medical device procurement; hazard vulnerability analysis incident response training; detection and analysis; containment, eradication and recovery; and post-activity efforts.

## Digital Health Precertification Program

On June 19, 2018, the FDA released the second version of its Pre-Certificate (Pre-Cert) Working Model that takes into consideration comments received on the April 2018 version. The agency accepted comments on the model until July 18, 2018. The goal, as outlined in the agency's Digital Health Innovation Plan, is to develop a voluntary Pre-Cert program that would facilitate faster review of certain product submissions from pre-approved software and digital health firms and developers. The initial pilot program has been limited to software as a medical device (SaMD), but the second version of the framework indicates FDA may extend the program to software in a medical device (SiMD) and accessories to medical device hardware in the future. Pre-Cert 1.0 may be released as early as the end of 2018 with anticipated pilot testing in 2019.

## Partnerships With Ethical Hackers

The FDA has recently pursued partnerships with ethical hackers in order to improve cybersecurity efforts with medical devices. This was highlighted by the recent discovery of a flaw in a Medtronic pacemaker that rendered the device vulnerable to hacking. Two cybersecurity researchers initially found the flaw and brought it to Medtronic and FDA's attention. In a statement to the media, the director of the FDA's CDRH indicated the FDA plans to continue developing relationships with cybersecurity researchers.

## Promoting the Use of Artificial Intelligence

FDA is moving toward approval of medical devices with artificial intelligence (AI), and Commissioner Scott Gottlieb indicated in a speech earlier this year that the agency is working to develop "a new regulatory framework to promote innovation in this space and support the use of AI-based technologies." Recent approvals by the agency have included a diagnostic system for diabetic retinopathy, clinical decision support software for strokes and a program to assist medical professionals in detecting wrist fractures. A noteworthy characteristic of the approved diabetic retinopathy diagnostic system is that it does not require any additional layer of review by a medical professional. Future approvals could work in coordination with the Pre-Cert program.

For more information about this topic, please contact one of the individuals listed in this publication.

## Contacts

**Elliot R. Golding**
Partner, Washington DC
T +1 202 457 6407
E elliot.golding@squirepb.com

**John E. Wyand**
Senior Partner, Washington DC
T +1 202 626 6676
E john.wyand@squirepb.com

**Jennifer M. Tharp**
Associate, Cleveland
T +1 216 479 8537
E jennifer.tharp@squirepb.com