King & Spalding
Client Alert

FEBRUARY 5, 2021

FDA and Life Sciences

FDA Appoints Renowned Cybersecurity Researcher to Head Agency's Medical Device Cybersecurity Efforts

For more information, contact:

Eric Henry
Washington, D.C.
+1 202 661 7823
ehenry@kslaw.com

Kyle Sampson
Washington, D.C.
+1 202 626 9226
ksampson@kslaw.com

Steven Niedelman
Washington, D.C.
+1 202 626 2942
sniedelman@kslaw.com

Lisa Dwyer
Washington, D.C.
+1 202 626 2392
ldwyer@kslaw.com

Elaine Tseng
San Francisco
+1 415 318 1240
etseng@kslaw.com

Earlier this week, FDA's Center for Devices and Radiological Health (CDRH) announced the appointment of Professor Kevin Fu, Associate Professor at the University of Michigan, as the Center's first Acting Director of Medical Device Cybersecurity, which portends increased focus on cybersecurity issues. The appointment of Dr. Fu is for one year, to serve on an acting basis, and includes responsibilities in CDRH's Digital Health Center of Excellence.

Professor Fu is highly credentialed, with B.S., M.Eng. and Ph.D. degrees from the Massachusetts Institute of Technology (MIT). He co-authored the seminal, well-publicized paper on the cybersecurity vulnerabilities inherent in implantable cardiac defibrillators (ICDs) — "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses" (2008). That paper brought the possibility of malicious attacks on connected medical devices to the attention of the industry, FDA, and the public. It was a primary motivator for an increased sense of urgency to address cybersecurity issues across the sector.

For more than 15 years, Professor Fu has been an outspoken champion of increased cybersecurity awareness and the implementation of best practices to protect medical devices and the patients that depend on them. While serving as Associate Professor at the University of Massachusetts Amherst, he founded the Archimedes Center for Healthcare and Device Security and worked as a visiting scientist at Microsoft, FDA's CRDH, and MIT. Professor Fu has testified before both houses of the U.S. Congress on medical device cybersecurity, and he has served in advisory roles to a number of federal agencies.

This appointment is widely seen by cybersecurity experts as an indicator of FDA's increased commitment to advance its regulatory guidance priorities. This includes updating its premarket cybersecurity guidance and guidance on the content of premarket submissions for software contained

in medical devices, both of which FDA has identified as “A-list” priorities for issuance in FY 2021. It will also increase the technical level of scrutiny the Agency applies to premarket product evaluations and facility inspections.

We are issuing this Client Alert to make industry aware of the potential for new and revised guidances associated with cybersecurity issues, as well as the possibility that an enhanced level of FDA oversight may be applied to medical devices. We will keep you apprised through additional Client Alerts as new guidances are finalized or issued. We have substantial capabilities and resources to provide expert assistance evaluating your current procedures, and helping to implement and execute any new guidances.

King & Spalding provides its clients with deep cybersecurity expertise to address this ever-changing regulatory landscape. Our FDA & Life Sciences Team employs more than 40 lawyers and consultants who have held senior positions in government, industry, academia and the medical profession. Our team includes Eric Henry, a Senior Consultant with 30 years of industry experience addressing software quality and medical device design controls (including cybersecurity, software-as-a-medical device (SaMD) and embedded software practices) in global leadership roles at Philips, GE Healthcare, Medtronic and Boston Scientific. Eric is available to provide assistance to our clients and to address any questions or needs they may have, including with respect to anticipating and addressing cybersecurity issues in FDA inspections, premarket submissions and postmarket management of medical devices (e.g., legacy technologies).

The King & Spalding Data Privacy and Security Practice further counsels clients on a broad range of legal issues faced by multinational organizations, including global privacy programs, data protection and cybersecurity assessments, crisis management in responding to internal and external privacy and data security incidents, health information governance and compliance, and defending clients in regulatory enforcement proceedings and class action litigation. The team consists of “boots on the ground” crisis managers, technical professionals, former government lawyers and litigators to manage and coordinate fast-moving and complex investigations and logistics during and after an incident. We assist clients with preparing for, responding to and recovering from data privacy and security incidents.