FDA U.S. FOOD & DRUG ADMINISTRATION
CENTER FOR DEVICES & RADIOLOGICAL HEALTH

Summary of the Patient Engagement Advisory Committee
September 10, 2019

Introduction:

The Patient Engagement Advisory Committee to the Food and Drug Administration (FDA) met September 10, 2019, to discuss and make recommendations on the topic "Cybersecurity in Medical Devices: Communication That Empowers Patients." Medical devices are increasingly connected to the internet, hospital networks, and other medical devices to provide features that improve healthcare and increase the ability of healthcare providers to treat patients. These same features may also increase cybersecurity risks. Preserving the benefit of these devices requires continuous vigilance as well as timely and effective communication to medical device users about evolving cybersecurity risks. The recommendations provided by the committee will address which factors should be considered by FDA and industry when communicating cybersecurity risks to patients and to the public, including but not limited to the content, phrasing, the methods used to disseminate the message and the timing of that communication. The recommendations will also address concerns patients have about changes to their devices to reduce cybersecurity risks as well as the role of other stakeholders such as healthcare providers in communicating cybersecurity risks to patients.

Presentations:

Norman "Ned" Sharpless, M.D., Acting Commissioner, FDA, welcomed the committee and public and provided opening remarks.

Michelle Tarver, M.D., Ph.D., Director, Patient Science & Engagement Program, FDA, provided updates on the Patient Science and Engagement Program.

Seth Carmody, PhD, Cybersecurity Program Lead, Office of Strategic Partnerships & Technology Innovation, CDRH, FDA, presented Medical Device Cybersecurity: A Total Product Lifecycle Approach.

Guest Speaker, Kevin Fu, Ph.D., Associate Professor, The University of Michigan, presented on Cybersecurity and Medical Device Updates.

Guest Speaker, Christian Dameff, M.D., University of California San Diego presented on the Physician Perspective on Cybersecurity.

Guest Speaker Jay Radcliffe, Thermo Fischer Scientific, presented on Cybersecurity Vulnerabilities.

Jodi Duckhorn, Acting Deputy Director, Office of Communication and Education, CDRH, FDA, presented on CDRH Communication of Medical Device Vulnerabilities and Safety Concerns.

Guest Speaker Catina O'Leary, PhD, LMSW, President/CEO, Health Literacy Media, presented Cybersecurity Vulnerability Communication.

Nastassia Tamari, Associate Director, Cybersecurity Incident Response, Becton Dickinson (BD) presented the Industry Perspective on Cybersecurity Communication.

Guest Speaker Karen McChesney, Juvenile Diabetes Research Foundation (JDRF), presented the Patient Perspective on Cybersecurity Communication.

Open Public Hearing:

Eleven open public hearing speakers presented and provided comments. Speakers included patients, research organizations, industry, patient advocacy groups and other members of the public.

Round Table Discussions:

During the roundtable discussion the audience was asked to discuss amongst their table a theoretical scenario regarding a cybersecurity safety concern associated with a medical device. Concluding the scenario discussion, FDA representatives presented comments generated by the audience.

Open Public Comment:

Ten Open Public Comment speakers provide comments on the roundtable discussions.

FDA Questions and Committee Discussion:

The Committee discussed approaches FDA and industry should consider in conveying cybersecurity risks to patients when the probability of exploitation is not known. The Committee believes in 1) the importance of timely communication; 2) a proactive view of pushing messages out; and 3) FDA's power to regulate and convene many stakeholders to discuss tactics to distribute messages. The Committee also believes that visual displays should be included in communication. Frequent

communication from FDA, as well as, other trusted sources should also be used to communicate risks. The expectations that FDA sets for manufacturers to communicate messages to patients, regardless of the patients' socioeconomic status, location, is important. Manufacturers look to FDA for the standards to use to communicate to patients. FDA should set those standards and hold the manufacturers accountable for the standards. The committee also believes that patients should have a choice on receiving information. Patients should receive information about a potential risk to the device early in the process. If it is a serious threat, the patient may want to be notified immediately. However, if it is a general update, the patient may not want to be notified. Patients should be able to have input on the level of communication they receive, as well as, the method in which they receive it.

Overall, the committee generally believes that there is not a blanket approach that would work for all patients. However, they highlighted 3 strategic elements that FDA and industry should consider in conveying cybersecurity risks to patients when the probability of exploitation is not known: 1) explaining the unknown factor; 2) FDA and industry understanding the fear of the potential unknown and having those concerns addressed and factored in well in advance of the preapproval process is important to patients and consumers; and 3) a balanced discussion between risk and benefits, highlighting the benefits especially if it is a lifesaving device. The committee also suggested that there is a need to use all mediums of communication as it pertains to communicating cybersecurity risk and the "particulars" matter regarding certain audiences or devices.

The Committee believes medical device cybersecurity is a matter of homeland and national security. The committee used the analogy of an airport security alert system or the stop light system of red, yellow, and green to help differentiate when something is actionable. They believe that these approaches provide clarity in a moment of fear and it conditioned the public to understand what actions to take with the different types of information being communicated. The Committee feels the FDA can use a similar system to communicate the different levels of cybersecurity threat so that the public knows how to understand the level of threat and what to do in response. In addition, the Committee generally believes that in some of the approaches FDA and industry use to communicate about other safety risks can be leveraged to communicate about cybersecurity, but there are additional communication considerations with cybersecurity. The committee recommends that FDA explore using Unique Device Identifiers (UDIs) to deliver targeted risk messages to patients who use a given device with a cybersecurity threat. FDA should also consider stakeholder engagement that involves consumers and patients who can help inform the messaging and the method of dissemination prior to a threat or cybersecurity risk.

As it pertains to additional information health care providers should have available to aid their discussion of benefits and risks with patients, the Committee feels that the FDA should consider the

burdens already placed on the providers. Trust is a critical factor in a cybersecurity conversation between physicians and patients and that patients would likely trust others on the physician's team. The committee believes that the technical experts that know the device well versus the prescriber of the device should include cybersecurity in their discussions with the patients. Training should be appropriate for the device and the person responsible for providing the training should be clearly identified. The Committee also feels that once an event happens, there should be some clear guidance on how it should be tracked, and how those impacted are identified and notified of the risk.

Overwhelmingly, the committee believed that it was important patients hear about a cybersecurity threat even before there was a risk reduction measure available. They felt it was important for transparency as well as to have patients become agents of detecting potential harms as part of the "ground intelligence system". The committee stated that the level of communication contributes to the credibility of an institution. In terms of the timing, FDA must also consider there are people who monitor the news to get information on vulnerabilities with the specific intent to exploit them. FDA could inadvertently trigger "bad actors" taking advantage of the risk if the communication of the risk is not well thought through before it is shared publicly (which the committee thought could be mitigated by only disclosing to the patient and not the public). FDA should also consider the cultural distinctions as it pertains to communications. The committee discussed the importance of the manufacturers in communicating cybersecurity threats to the patients, giving them the option of an "opt-out" feature or a way to only hear about patches or updates when they need to take an action. The level of communication should be determined by the level of the threat, the targeted population, and the timeliness of information should also be considered. The committee felt that the type of device, whether it's implanted, wearable or a connected device was a secondary concern, the primary concern is informing patients at the right time. The committee believes there should be a certification requirement on device cybersecurity offered to local individuals who care for patients such as the clinical staff and community health workers. In addition, the committee suggested a cybersecurity hygiene course be created for the specific device and offered online with the frequency of the training being determined by the type of device.

The Committee generally believes that knowledge does not necessarily confer responsibility and that the burden should not be put on the patient to find the information pertaining to risks or threats associated with their device(s). FDA should make sure that burden is on industry to communicate the risk and not pushed back on patient to find it. Industry and others involved need a standard on how they communicate to patients. The Committee also believes FDA should use a collaborative method to communicate messages to patients. FDA, industry, health care systems, patient safety organizations, professional societies, and public-private partnerships should all

contribute to developing resources to communicate messaging. The committee highlighted that the manufacturers, health care providers, and hospital systems are critical in developing and disseminating the messages. The committee emphasized the importance of patient advocacy groups to help in the development and dissemination of the messages. In addition, the committee thought that updates and patches should follow a healthy choice architecture where the "healthier option" is the default.

The Committee generally believes FDA should use their authority to ensure patients safety by developing standards and holding manufacturers accountable to the standards around communicating medical device cybersecurity. The Committee agrees that the format in which messages are conveyed should include e-mails, web posting, social media and webinars. There should be a high standard of outreach to all patients regardless of the challenges with reaching them since connectivity will be increasing with time and those populations in rural or internet sparse areas will become increasingly vulnerable to cybersecurity threats. The Committee recommends the FDA look at the high standards that the Department of Transportation and other transportation agencies use to hold high standards for manufacturers across their supply chains and the FDA should consider some of the mandates the transportations agencies use to communicate risks to their passengers. The committee reinforced that FDA's roles is to protect the consumer and to hold the manufacturers accountable for the device they own, ensuring the manufacturer takes responsibility for their device.

Contact:
Letise Williams, Designated Federal Officer
301-796-8398, Letise.Williams@fda.hhs.gov

Transcripts may be purchased from: (written requests only)
Free State Reporting, Inc.
1378 Cape St. Claire Road
Annapolis, MD 21409
410-974-0947 or 1 800-231-8973 Ext. 103
410-974-0297 fax
Or
Food and Drug Administration
Freedom of Information Staff (FOI)
5600 Fishers Lane, HFI-35
Rockville, MD 20851
(301) 827-6500 (voice), (301) 443-1726