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

U.S. Food and Drug Administration (FDA)
Center for Devices and Radiological Health (CDRH)
Patient Engagement Advisory Committee (PEAC) Meeting
Holiday Inn Gaithersburg

FDA DISCUSSION QUESTIONS

SEPTEMBER 10, 2019

OVERVIEW

As discussed in the Executive Summary, communicating health risk information is complex. Integrating an assessment of medical device cybersecurity risk into health risk communication adds another dimension to the complexity because cybersecurity contains certain unknowable elements. In addition, one may not be able to leverage historical data sets or prior evidence-based materials to calculate probabilities, as may be used for other device-related safety concerns.

With medical device cybersecurity, FDA often considers the following factors when considering whether to release a safety communication to the public:

- the unknowable probability of successful exploitation of a device;
- the speed and spread with which an exploit may occur along with its impact across the patient population; and
- the time it would take to put in place (deploy) an effective countermeasure that contains and mitigates harm (generally outpaced by the speed and scale of the exploit's impact).

For these reasons, FDA's communication approach regarding medical device cybersecurity has been anticipatory, forward-leaning and proactive as vulnerabilities are identified and verified *before* exploitation, and when there is a mitigation available, rather than waiting for a signal or indicator of harm to manifest.

In addition, the general challenges with communicating health risk information are amplified by the following considerations related to medical device cybersecurity risks:

- Lack of public awareness about cybersecurity risks,
- The role of users in the application of timely updates and patches,
- Questions about when to communicate,
- Qualification/quantification of cybersecurity risks,
- Providing actionable information,

- Determining the exploitability of a vulnerability, and
- Determining the impact of an exploit.

QUESTIONS

1. In general, for most safety messages (and specifically, those outside of the realm of cybersecurity), FDA communicates the types of harms that may result from a medical device malfunction or failure and their associated likelihood of occurring, if known. Unlike other medical device safety concerns, the probability of a successful exploitation of a medical device cyber vulnerability is not knowable. This challenge can impede informed decision making between patients and health care providers in determining whether the benefits of a patient taking actionable steps to reduce the potential for harm (should the vulnerability be exploited) outweighs the potential risks related to deploying the cybersecurity fix (such as software updates that have a quantifiable failure rate).
    a. What approaches do you think the FDA and industry should consider in conveying cybersecurity risks to patients when the probability of exploitation is not known?

    b. Is this suggested approach similar to or different from how the FDA and industry should communicate about risks other than cybersecurity? Please explain.

    c. What additional information do you think health care providers should have available to aid their discussion of benefits and risks with patients?

2. In general, when FDA determines through its assessment of the vulnerability and severity of clinical impact that risks to the patient are unacceptable and there is a way to reduce those risks, the FDA will communicate. Regarding the timing of communication, the cybersecurity community holds varying views for when to communicate risks in safety-critical industries, such as the medical device sector. A prevailing perspective to which FDA adheres is that in the absence of an effective way to reduce risk, prematurely communicating can increase the opportunity for exploitation by highlighting a potentially unknown issue and, by extension, increasing the potential exposure to harm.

    A definitive fix of a vulnerability can take weeks to many months to develop and test before it can be deployed safely. While such a permanent solution (such as a software update) is being developed, risk reduction measures are recommended. It is important to note that such risk mitigations can potentially introduce other risks (such as stopping the use of a device that is beneficial to the patient) and such mitigations are often intended to only be temporary solutions (such as disconnecting from the internet).

   a. What do you think the FDA should consider as the “trigger” to communicate about medical devices affected by a cybersecurity vulnerability:
      i. When the FDA identifies a vulnerability, even if no risk reduction measure is available;
      ii. When there is an action for patients to take or a risk reduction measure available; or
      iii. Other (please elaborate)?
   b. Would your recommendations change if the device was:
      i. implanted (such as a defibrillator or deep brain stimulator),
      ii. connected (such as an infusion pump), or
      iii. worn (Continuous Positive Airway Pressure (CPAP) machine)?

3. There are best practices in cybersecurity which should be performed to maintain the security of connected devices. These include, but are not limited to: enabling, setting, and changing passwords; keeping software and applications up-to-date with the most recent versions; and not opening suspicious emails.

   Should patients receiving new medical devices be educated about the functionality, security elements and cybersecurity of the device including the importance of security maintenance over the device’s lifetime (often called cybersecurity hygiene) when the device is prescribed?

   a. What, if any, existing resources are available to patients to help inform this dialogue?
   b. If new resources need to be developed, who do you think should develop these educational resources (industry, FDA, health care systems, patient safety organizations, professional societies, public-private partnerships, others)?
   c. How might these resources be best disseminated to attain universal patient access?

4. What other recommendations do you have about the FDA’s communication approach for medical device cybersecurity? How do you believe patients want to receive information about medical device cybersecurity from the FDA? Please consider each of the following:
   a. Designating information that is actionable versus information for awareness;
   b. Tailoring and distributing message content to multiple audiences (for example, patients, health care providers, industry);

   c. The format in which the information is conveyed (such as email, web posting, and social media); and
   d. Frequency with which the message is reinforced.

5. Hard-to-reach populations include those in rural or other areas with limited access to health care providers or facilities, or limited access to the internet and other wireless technologies.
   a. What do you recommend the FDA, patient organizations, industry and health care providers do to disseminate information about medical device cybersecurity issues to these populations?
   b. What other organizations or groups could partner with other stakeholders to facilitate communication with these populations?
   c. Who is responsible for ensuring hard-to-reach patients receive the messages?