FDA 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

CYBERSECURITY SCENARIO

September 10, 2019

You are a patient with an irregular heartbeat. Your doctor recommends that you have Device C surgically implanted in your heart to make your heart beat regularly. Device C has completely changed how physicians treat your condition and has significantly increased survival rates. Device C can be monitored wirelessly or by the telephone. Because Device C is a wireless device, it is vulnerable to unauthorized outside interference.

Q1: Would you expect your health care provider to discuss the cybersecurity risks associated with Device C during the informed consent process before surgery? Why or Why not?

Q2a: Would the possibility of your device being vulnerable to unauthorized outside interference change your decision to have Device C implanted?

Q2b: If yes, would you ask your health care provider what the alternatives are to Device C and if there are other similar devices that are considered more secure?

Q2c: Would you want to weigh the benefits and risks of implanting a device versus managing your irregular heartbeat with medication?

You choose to have Device C implanted to make your heart beat regularly. Five years later, while on a social media site, you read a post where someone claims that they have figured out how to interfere with devices like Device C.

Q3: What would you do after seeing this information?

Q4: Where would you look to find additional information about the vulnerability concerns of these types of devices?

One month later at your next scheduled visit with your health care provider, you ask whether Device C specifically could stop functioning due to interference by non-medical personnel. Your health care provider confirms that it is possible.

Q5: What would you expect your health care provider to communicate to you about any potential risks?

Q6: Do you think your health care provider should be the main point of contact to educate you about the cybersecurity risks associated with Device C? Would you expect/want to receive information from anyone else besides your health care provider?

Six months following your clinic visit, the FDA and the device manufacturer communicate safety messages about threats and vulnerabilities associated with Device C. An excerpt from the disseminated message is shown below:

Company XYZ has planned an upgrade to the firmware installed on Device C. This firmware upgrade will improve performance and strengthen the security of this device. The security update provides an additional layer of protection against unauthorized access to your device. Unauthorized access could prevent delivery of appropriate therapy. The update is intended to prevent anyone other than your doctor from changing your device settings.

What do I need to know about the update process?

You should have a conversation with your physician to determine if the firmware upgrade is right for you. If you and your physician decide that it is, the firmware upgrade will take approximately 5 minutes to complete and the device will operate in its backup mode during this time. There is a small chance (<1%) that the firmware update process might not be successful, and your device will need to be replaced through a routine surgical procedure.

You should have a conversation with your physician to determine if the firmware upgrade is right for you. If you and your physician decide that it is, the firmware upgrade will require placing a disk over the device. During the upgrade process, a disc will be placed over Device C and will transfer information to Device C. The upgrade process typically takes approximately 5 minutes to complete.

Q7: From whom would you expect to hear information about the safety concerns associated with Device C? What sources (people, websites, organizations) would you consider trustworthy for relaying safety information and recommendations associated with Device C?

Q8: Do you think more routine general messaging on cybersecurity risks and safety precautions would raise awareness of cybersecurity with medical devices? Who should communicate that information? Where and in what format would you expect that information?

You are concerned about the risks associated with the upgrade, which include stopping the function of the device and breaking the device, requiring another surgical procedure to replace it. In your discussion with your health care provider, you talk about the cybersecurity risks and whether it is worth the risk of the upgrade. The risk of the upgrade breaking Device C and rendering it non-functional is unknown and the potential cybersecurity risk leading to death if the vulnerability is left unaddressed is not presently quantifiable.

Q9: How would you weigh the benefits of upgrading Device C against the risks of the upgrade? Would you decide to upgrade?