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

Communicating Cybersecurity Vulnerabilities to Patients: Considerations for a Framework

DISCUSSION PAPER AND REQUEST FOR FEEDBACK

PATIENT ENGAGEMENT ADVISORY COMMITTEE

October 2020

Preamble

The U.S. Food and Drug Administration's (FDA's) Center for Devices and Radiological Health (CDRH) has developed *Communicating Cybersecurity Vulnerabilities to Patients: Considerations for a Framework* to provide best practices to consider when communicating with patients and caregivers about cybersecurity vulnerabilities. Although it may not be possible to communicate about every cybersecurity vulnerability, the FDA works with federal partners and industry stakeholders to assess the best approaches to communicate with patients and caregivers about specific and relevant cybersecurity events that may affect public health. *Communicating Cybersecurity Vulnerabilities to Patients: Considerations for a Framework* outlines considerations for the FDA, federal partners, and industry stakeholders to help thoughtfully inform patients and the public about cybersecurity vulnerabilities.

Communicating Cybersecurity Vulnerabilities to Patients: Considerations for a Framework is being issued for discussion purposes only and is not a draft guidance. This document is not intended to communicate the FDA's proposed (or final) regulatory expectations but is instead meant to seek early input from groups and individuals outside the Agency.

Contents

Background

The U.S Food and Drug Administration's (FDA's) Center for Devices and Radiological Health (CDRH) remains committed to its mission to promote and protect the public health, including the safe and effective use of medical devices that are connected to the Internet, hospital networks, and other medical devices (hereafter referred to as "connected medical devices"). These medical devices range from sensor-based technologies such as wearables, to implantable medical devices, such as pacemakers. The increased use of connected medical devices in the United States has led to an increase in cybersecurity vulnerabilities. The FDA is at the forefront of helping mitigate cybersecurity issues related to the use of connected medical devices. Currently, the FDA's safety communications fall into two main categories: device-specific information and underlying technology issues. The FDA tailors its communications depending on the specific audiences (such as patients, healthcare providers, and industry) and the communication type (such as safety or educational communications). The FDA also tailors its communications based on the urgency of the issue and the public health impact. The FDA acts promptly to communicate on cybersecurity vulnerabilities with the public to ensure they are aware of these issues and have the information they need to take appropriate action. Clear, actionable communication is one way to help protect and promote public health, and helps ensure that patients, who depend on their medical devices, stay informed and protected.

The Patient Engagement Advisory Committee (PEAC or the Committee) provides advice to the Commissioner or their designee on complex, scientific issues relating to medical devices, the regulation of medical devices, and their use by patients. The PEAC may consider topics such as Agency guidance and policies, clinical trial or registry design, patient preference study design, benefit-risk determinations, device labeling, unmet clinical needs, available alternatives, patient-reported outcomes, and device-related quality of life or health status issues. The Committee provides relevant skills and perspectives, in order to improve communication of benefits, risks, clinical outcomes, and increase integration of patient perspectives into the regulatory process for medical devices.[1]

During the PEAC meeting on September 10, 2019, the members expressed the importance of clearly and consistently communicating about cybersecurity vulnerabilities, as well as clearly identifying when patients need to take an action to mitigate potential harms. These findings are shared in the Summary

[1] More information about PEAC can be found at: https://www.fda.gov/AdvisoryCommittees/CommitteesMeetingMaterials/PatientEngagementAdvisoryCommittee/default.htm

of the Patient Engagement Advisory Committee document. The FDA's Internal Message Testing Network (for which participants serve as a proxy for the public) also reviewed four cybersecurity messages created by the FDA and manufacturers. This review provided insights on how the FDA and potentially other stakeholders in the field of cybersecurity vulnerability communications could tailor approaches for communicating about cybersecurity vulnerabilities with patients and caregivers. The feedback from these stakeholders is the foundation for the development of this document.

Goals

The FDA is holding its next PEAC meeting on October 22, 2020 and has developed this discussion paper to provide potential best practices and elements to consider when developing a cybersecurity communication framework. These elements include:

- interpretability;
- discussing risks and benefits;
- acknowledging and explaining the unknown;
- availability and findability of information;
- structure of the communication material; and
- outreach and distribution vehicles.

The FDA seeks further input from patients, patient advocacy organizations, the medical device industry, clinical researchers, and others on this topic. The FDA intends to use this feedback to inform future efforts designed to improve cybersecurity safety communications, including the potential development of a cybersecurity communications framework. In particular, the FDA seeks further comment from the public on the following questions:

1. Are the elements outlined as part of the considerations for a framework the most appropriate and relevant for effective communication about cybersecurity vulnerabilities with patients and the public?

2. Are there any elements that are missing, or that could be strengthened or clarified to help develop a useful framework?

Important Elements to Consider

The feedback received at the 2019 PEAC Meeting and through the FDA's Internal Message Testing Network highlighted important elements to include in the development of safety communications for cybersecurity vulnerabilities. Such elements include interpretability, discussing risks and benefits, acknowledging and explaining the unknown, availability and findability of the information. This document expounds on these elements, which comprise the considerations that may inform a potential future communications framework for cybersecurity vulnerabilities. These elements are discussed below with an example of how these elements might be applied (**Appendix**).

Interpretability: Make it Easy for People to Read and Understand

When developing safety communications, it is important to consider the messenger's need to communicate the messages in clear and plain language with the audience's need to receive and understand the message conveyed. Throughout this document, messengers may include the FDA, other federal agencies, and industry; the audience may include patients and caregivers. Several factors, such as timeliness, relevance, simplicity, and readability for diverse audiences are key for patients and caregivers to read and understand the safety communications.

Keep it Timely

Whenever possible, communicate with patients and caregivers as early as possible, especially if the cybersecurity vulnerability presents a serious threat. Early access to serious cybersecurity vulnerability information may provide assurance to patients and empower them to take early action to avoid any potentially harmful consequences to their health. Furthermore, early access to this information may also help build trust with patients and the public.

Keep it Relevant

Patients and caregivers have indicated that communicating risk and urgency are important to them. Clearly explaining the risks near the top of the safety communication and stating the urgency of the risk is one way to help emphasize critical information to the audience. It is also important to have a call to action (i.e., clear actions that patients and caregivers can take) so that patients and caregivers know what steps to take to mitigate those risks if possible. In some cases, it may not be possible for patients to mitigate risks, as an update to their device may not yet exist, or they may need to wait for the medical device manufacturer, healthcare provider, or other party to take some action first. In these cases, it may be helpful to clearly outline what patients can and cannot do. The communication should

provide clear and concise instructions for recommended actions and focus on what patients and caregivers should do.

One way to help ensure communications are relevant is to conduct message testing with target audiences. Organizations may want to consider having patient advisory boards that could assist with message refinement.

Keep it Simple

To best reach your target audience, it is helpful to communicate about cybersecurity vulnerabilities in the simplest way possible. Using terminology that your target audience understands is a best practice in communications, and pilot testing the communication with your audience can help you better assess what they do and do not understand (Centers for Disease Control and Prevention, 2019). When developing safety communications, it is helpful to avoid the use of technical language and jargon and avoid acronyms or, if acronyms are necessary, spell them out when they first appear. If some degree of technical jargon is necessary, it can be helpful to provide plain language explanations of the jargon in the same sentence in which the terminology is introduced or immediately following. One form of technical jargon may include the name of the cybersecurity vulnerability. The FDA's Internal Message Testing Network found that the target audience confused the name of the vulnerability with the name of the device. It would help patients if the communications clearly explain the difference between the name of the vulnerability and any affected medical devices.

Keep it Readable for Diverse Audiences

While keeping it simple will help enable all audiences to better understand the communication, it is also important to ensure that the information is available to diverse readers in their preferred language. Providing translation services for relevant languages may increase the number of people who read and understand the communication. For instance, if a specific issue targets elderly Hispanic and Latinx patients that may primarily speak Spanish, it may help reach the target audience if the safety communication was available in Spanish. Language translation is not simply writing text in another language, but also includes considering the cultural nuances of speech when crafting the message. Due to the nuances of cybersecurity communications and regulatory language, using machine translations is not a best practice, as these translators may not capture the subtleties of the language and may misinform or confuse the reader.

Discuss Risks and Benefits

During the PEAC meeting, the Committee stated that it was important for messengers to convey a balanced discussion between the risks and benefits when the probability of cybersecurity exploitation remains unknown. In particular, the Committee recommended a "balanced discussion between risk and benefits, highlighting the benefits especially if it is a lifesaving device" (Summary of Patient Engagement Advisory Committee, 2019). When discussing cybersecurity vulnerabilities, if there are risks associated with mitigations, it is important to discuss both the risks and benefits of actions related to addressing the specific vulnerability. The goal is to help provide patients and caregivers information about their options when deciding to act or not act on a specific issue or call to action.

Acknowledge and Explain the Unknown

If something is not known at the time of the communication, consider acknowledging and explaining to the audience the unknown information so that this is not perceived as an omission (intentional or unintentional) or an oversight. This will also help the reader have confidence that the information is accurate and trustworthy. For instance, if there is a vulnerability detected for a device, but that device has no means by which to detect whether the vulnerability has been exploited, it is important to note that there are "no known exploits at this time," rather than "no exploits," as it would be impossible to state there were no exploits with certainty.

Availability and Findability: Make it Easy for Patients to Find and Use

As noted in the Summary of the Patient Engagement Advisory Committee (PEAC) from September 10, 2019 (Summary of Patient Engagement Advisory Committee, 2019):

> "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."** (emphasis added)

The FDA and industry share responsibility for communicating about cybersecurity risks in medical devices to patients and caregivers in a manner that is easy to find. The elements below expound upon the best practices of availability and findability, which include more considerations for a potential future communications framework for cybersecurity.

Make Communications Easy to Find in Online Searches

Numerous studies have shown that patients use internet searches to find health information. (Diaz, et al., 2002) (Madrigal & Escoffery, 2019). Online search engines drive a large proportion of visits to the FDA's safety communications. In addition, patients and caregivers may hear about cybersecurity vulnerabilities before receiving an alert from a device manufacturer and may attempt to search for more information using an internet search.

Safety communications on cybersecurity risks are more easily found if they incorporate best practices in search engine optimization (SEO) techniques, such as:

- including the name of the manufacturer and device name (or device category name) in the title of the communication, if the cybersecurity vulnerability is specific to a medical device or group of medical devices;
- including other important keywords that patients may search for near the beginning of the title, such as the name of the cybersecurity vulnerability; and
- incorporating important keywords in the content itself, including the list of specific medical devices, as well as the associated diseases or conditions.

Feedback from the FDA's Internal Message Testing Network indicated a patient preference for including medical device names in the title of the communication. This feedback also indicated that including the name of the vulnerability in the title was often confused with the medical device name. For findability purposes, it is important to include the name of the cybersecurity vulnerability in the title. Hence, a clear presentation of how names are used is critical to patient and public understanding and identification.

Make Communications Easy to View on Mobile Devices

According to the Pew Research Center (Mobile Fact Sheet, 2019), the vast majority of adults in the United States (96 percent) own a smartphone of some kind, and 37 percent of U.S. adults surveyed (Anderson, 2019) mostly use a smartphone when accessing the Internet. For certain groups, such as younger adults and adults without a broadband connection at home, that percentage is even higher. Metrics for mobile access of the FDA's safety communications show that, depending on the topic, most visitors are using mobile devices to read the information (Unpublished Data, 2020).

For these reasons, safety communications on cybersecurity risks may be more effective if they incorporate best practices for mobile-friendly content. The FDA adopted a mobile-friendly, responsive design approach to its web content in 2013. Some mobile-friendly best practices include:

- Chunking content for easy scanning by using sub-headers, lists, bullets, simple tables, and other formatting techniques;
- Using brief paragraphs and short titles that are easier to read on a smaller screen; and
- Following the plain language principles described above in the *Interpretability* section.

Mobile-friendly designs and writing techniques also enhance findability, since search engines rank mobile-friendly content higher in search results pages (Uzialko, 2020).

In addition, making communications accessible for individuals with disabilities will enable these audiences to better access cybersecurity vulnerability communications. All federal agencies must comply with Section 508 of the Rehabilitation Act, which "require[s] federal agencies to make their electronic and information technology (EIT) accessible to people with disabilities" (IT Accessibility Laws and Policies, 2020).

Communication Structure

Information hierarchy is essential to safety communication structure. It is important for patients and caregivers to quickly find information relevant to them. Thus, it is important for safety communications to lead with the main message and recommendations for patients and caregivers.

Good organization is also an important factor when constructing safety communications. Consider your audience and put clear and succinct messages that are most relevant to patients and caregivers at the top, near the beginning of the safety communication. The FDA's Internal Message Testing Network showed a preference for communications that are short. Include information about specific diseases or affected medical devices, as applicable, at the top of the communication.

Additionally, providing visual cues, such as simple tables, call out boxes, *italics*, and **bolded text**, among others, to draw the reader's attention to the main message can be beneficial to craft a message that is compelling and palatable to lay audiences. For instance, grouping information about one disease or device in the same section (such as diabetes or pacemakers) could help readers better identify and understand the information.

Outreach and Distribution Vehicles

As with any important communication issues, having an outreach plan and developing appropriate communication channels help aid the comprehensive dissemination of information about safety communications, including cybersecurity vulnerabilities. Depending on the type of vulnerability, the messenger may need to conduct outreach with partner organizations to help inform the target audience. Different types of vulnerabilities and audiences may need different approaches, so it is important to consider which combination of distribution vehicles could be used to maximize outreach.

Outreach Plan

It is important for the outreach plan to consider the target audience, key messages, and distribution vehicles intended to reach the target audiences. When developing an outreach plan, consider the must-reach audience for the communication material and determine how best to assure they receive the message. These considerations may include age, race, ethnicity, language, geography, disease, device use, or any other identifying feature that could help inform approaches that might be effective at having the greatest impact. Advance planning for these types of communications is important, as is reaching the target audiences. Given the need to communicate quickly, it may be advantageous to develop ongoing relationships with outreach partners prior to an incident occurring. This planning may help ensure that when the time comes, these relationships are in place for rapid communication deployment. Creating a template for these types of communications may also enable faster communications.

Distribution Vehicles

There are many possible distribution vehicles to reach different audiences. Using a combination of different distribution vehicles may lead to the greatest dissemination of the communication materials. For example, if the affected device is specifically used for a condition impacting many African Americans and the Hispanic and Latinx population, then the distribution vehicles may need to be augmented to assure outreach to these populations. Just as language may be tailored for the target audience, and communications may be translated based on target audience, distribution vehicles may be tailored for the target audience. Each communication plan may consider the unique needs of the audience and tailor distribution vehicles based on how to best reach those patients.

The list below, while not comprehensive, reflects the distribution vehicles mentioned during the FDA's Internal Message Testing efforts and the 2019 PEAC meeting. It also reflects participants' thoughts on the utility and reliability of such vehicles.

- **Email and patient listservs** – Direct emails to patients or use a listserv (for instance to consumer and patients' groups or state, local, and territorial governments) to communicate with patients and caregivers is also an effective way to reach out your target audience. Participants found emails and listservs to be a reliable way of receiving information.
- **Text messages** – The use of a company-based text program has been used to reach target audiences to deliver safety information. Text message programs have been used for public health interventions, can be relatively inexpensive, and can be a direct channel to reach the target audience. As patients increasingly rely on cell phones for communication, text messaging can be an instantaneous communication vehicle that patients can read at their convenience (Wagner, 2019). Participants found text messages to be a reliable way of receiving information.
- **Social Media** –Recent research has shown that information quality and authority is a concern when people consider using health information from social media but that credibility may vary by type of social media channel (Zhao & Zhang, 2017). Although the use of social media is widespread, some of the participants indicated that they did not consider social media to be a reliable source of information as it may be perceived as spam (unsolicited digital communication sent out in bulk).
- **Television** – Participants also considered television to be a reliable source of information. Because this can be an expensive vehicle to deliver information, organizations could consider whether this is an appropriate and feasible vehicle for them.
- **Websites** – Government and private industry use their own websites to disseminate safety information. Whether organizations use safety alerts or other media vehicles (such as a press release or an in brief), they try to maximize this channel to deliver safety information. Although participants were not asked directly about their preferences for websites, the other distribution vehicles typically direct patients to websites to find more information. When applying best practices described above, websites can be an effective tool for communication.

Conclusion

Communicating about medical device safety is an important part of the FDA's work to ensure patient safety and the overall safety and effectiveness of medical devices. As the use of connected medical devices increases and cybersecurity threats to the healthcare sector have become more frequent, more severe, and more clinically impactful (U.S. Food & Drug Administration, 2018), it is increasingly

important for the FDA, industry, and other stakeholders to improve on cybersecurity safety communications. These considerations for a framework are a critical step to begin this improvement.

It is essential that communications be available, easy to find, and easy to understand. Additionally, it is critical for them to be timely, relevant, simple, and readable for a diverse audience, discuss the risks and benefits, and acknowledge any unknown information. Information about cybersecurity vulnerabilities is vital to share with patients and caregivers to help them make informed decisions about their health and their medical devices.

Appendix: Sample Cybersecurity Vulnerability Safety Communication

NOT REAL – MOCK-UP OF CYBER COMMUNICATION – NOT REAL

Your Brand X Insulin Pump May Be Affected by X Cybersecurity Risk

Medical devices, like other computer systems, can be vulnerable to security breaches, potentially impacting the safety and effectiveness of the device. These are ***cybersecurity risks***.

Contact your health care provider right away if you think your Brand X insulin pump settings or insulin delivery changed unexpectedly.

The FDA recommends people who have affected **Brand X** insulin pumps update the software on their devices to protect them from these risks.

An unauthorized person (someone other than a patient, patient caregiver, or health care provider) could potentially connect wirelessly to a nearby **Brand X** insulin pump. This unauthorized person could change the pump's settings to either over-deliver insulin to a patient, leading to low blood sugar (hypoglycemia), or stop insulin delivery, leading to high blood sugar (hyperglycemia) and diabetic ketoacidosis.

NOT REAL – MOCK-UP OF CYBER COMMUNICATION – NOT REAL

The FDA recommends people who have affected **Brand X** insulin pumps update the software on their medical devices to protect them from these risks.

> At this time, the FDA has not received any confirmed reports of unauthorized persons changing settings or controlling insulin delivery to **Brand X** insulin pumps.

Check to See if Your Insulin Pump Is Affected by X Cybersecurity Risk

Certain **Brand X** insulin pumps may be affected by this cybersecurity risk. People who have diabetes and use these models should update their insulin pump to the latest version of the device software to protect against these potential risks.

Read the **Brand X** Letter to Patients to learn how to identify your pump's software version.

If You Believe Your Insulin Pump May Be Affected by X Cybersecurity Risk:

- Talk to your health care provider if you believe your treatment has been affected.
- Update the software of your insulin pump to ensure more cybersecurity protection.
- If you have questions about updating your pump software, call **Brand X** at 1.800.555.1212 or email updatepump@BrandX.com or visit www.BrandX.com.
- Follow the steps listed below in "**Everyone With an Insulin Pump Should Take the Following Steps to Help Prevent the Risk of a Cybersecurity Attack**."

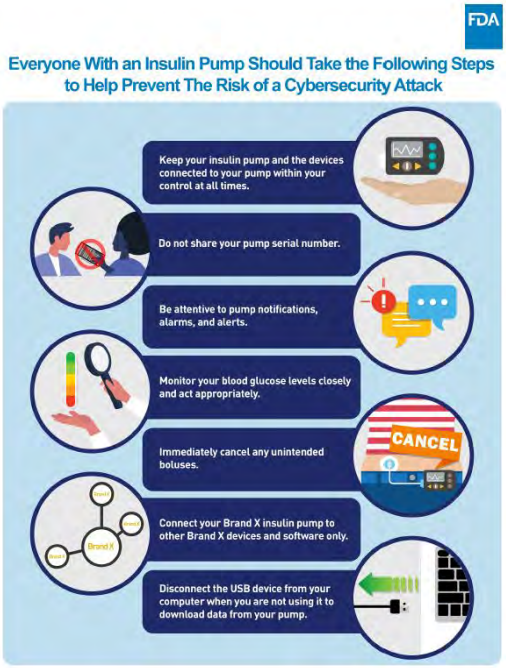
Get Medical Help Right Away if You:

- Have symptoms of severe hypoglycemia (such as excessive sweating, feeling very tired, dizzy and weak, being pale, and a sudden feeling of hunger).
- Have symptoms of diabetic ketoacidosis (such as excessive thirst, frequent urination, nausea and vomiting, feeling very tired and weak, shortness of breath).
- Think your insulin pump settings or insulin delivery changed unexpectedly.

NOT REAL – MOCK-UP OF CYBER COMMUNICATION – NOT REAL

Everyone With an Insulin Pump Should Take the Following Steps to Help Prevent the Risk of a Cybersecurity Attack:

- Keep your insulin pump and the devices connected to your pump within your control at all times.
- Do not share your pump serial number.
- Be attentive to pump notifications, alarms, and alerts.
- Monitor your blood glucose levels closely and act appropriately.
- Immediately cancel any unintended boluses.
- Connect your **Brand X** insulin pump to other **Brand X** devices and software only.
- Disconnect the USB device from your computer when you are not using it to download data from your pump.



Download image

Report Problems with Your Insulin Pump

Report any problems you have with your insulin pump to the FDA through the MedWatch Voluntary Reporting Form.

More Information

- **Brand X's** Letter to Patients.
- Cybersecurity: The FDA's webpage about cybersecurity risks and medical devices

The FDA will provide updates as new information becomes available.

Questions?

If you have questions, email the Division of Industry and Consumer Education (DICE) at DICE@FDA.HHS.GOV or call 800-638-2041 or 301-796-7100.

References

Anderson, M. (2019, June 13). *Mobile Technology and Home Broadband 2019*. Retrieved from Pew Research: https://www.pewresearch.org/internet/2019/06/13/mobile-technology-and-home-broadband-2019/

Centers for Disease Control and Prevention. (2019, August). *CDC Clear Communication Index: A Tool for Developing and Assessing CDC Public Communication Products User Guide*. Retrieved from Centers for Disease Control Web site: https://www.cdc.gov/ccindex/pdf/ClearCommUserGuide.pdf

Diaz, J. A., Griffith, R. A., Ng, J. J., Reinert, S. E., Friedmann, P. D., & Moulton, A. W. (2002, March 17). *Patients' Use of the Internet for Medical Information*. Retrieved from National Center for Biotechnology Innovation: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1495021/

IT Accessibility Laws and Policies. (2020, July). Retrieved from Section508.gov: https://section508.gov/manage/laws-and-policies

Madrigal, L., & Escoffery, C. (2019, March 21). *Electronic Health Behaviors Among US Adults With Chronic Disease: Cross-Sectional Survey*. Retrieved from National Center for Biotechnology Information: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6423466/

Mobile Fact Sheet. (2019, June 12). Retrieved from Pew Research: https://www.pewresearch.org/internet/fact-sheet/mobile/

Summary of Patient Engagement Advisory Committee. (2019, September 10). Retrieved from www.fda.gov: https://www.fda.gov/media/130778/download

U.S. Food & Drug Administration. (2018, October 18). *Food and Drug Administration*. Retrieved from Content of Premarket Submissions for Managment of Cybersecurity in Medical Devices: Draft Guidance for Industry and Food and Drug Administration Staff: https://www.fda.gov/media/119933/download

(2020). *Unpublished Data.* Silver Spring, MD: Food and Drug Administration.

Uzialko, A. (2020, January 5). *Why Your Wesite Needs to be Google Mobile-Friendly*. Retrieved from Business News Daily: https://www.businessnewsdaily.com/7808-google-search-ranking-mobile.html

Wagner, J. (2019, May 8). *Leveraging Text Messaging to Improve Communications in Safety Net Programs.* Retrieved from Center on Budget and Policy Priorities: https://www.cbpp.org/research/poverty-and-inequality/leveraging-text-messaging-to-improve-communications-in-safety-net

Zhao, Y., & Zhang, J. (2017). Consumer health information in seeking social media: a literature review. *Health Information and Libraries Journal*, 268-283.