



U.S. FOOD & DRUG
ADMINISTRATION

# Best Practices for Communicating Cybersecurity Vulnerabilities to Patients

Center for Devices and Radiological Health

October 2021

## Preamble

The U.S. Food and Drug Administration's (FDA's) Center for Devices and Radiological Health (CDRH) has developed *Best Practices for Communicating Cybersecurity Vulnerabilities to Patients* for industry stakeholders and federal partners to consider when designing a communication approach for 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.

*Best Practices for Communicating Cybersecurity Vulnerabilities to Patients* incorporates feedback received from the public on the earlier draft document *Communicating Cybersecurity Vulnerabilities to Patients: Considerations for a Framework* incorporating feedback from the public. This document is not guidance and does not create or convey any policies on regulatory matters or any regulatory expectations. In addition, the references cited herein are for informational purposes only and should not be construed as endorsements. We hope that this document may be a useful resource for industry stakeholders and federal partners as well as other stakeholders who may be communicating about cybersecurity vulnerabilities to patients and caregivers.

# 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 software as a medical device (SaMD) such as phone applications, 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 software and hardware supply-chain issues. The FDA tailors its communications depending on the specific audiences (such as patients, health care 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 help ensure that patients, who depend on their medical devices, stay informed and protected. We shared the challenge of communicating cybersecurity vulnerabilities with the Patient Engagement Advisory Committee (PEAC) for their recommendations for future communications.

The PEAC (referenced as the Committee) provides advice to the FDA 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 design and conduct, real-world data use, patient science, benefit-risk determinations, device labeling, and other general matters related to medical devices. 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 (U.S. Food and Drug Administration, 2020).

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 action to mitigate potential harms. These findings are shared in the Summary 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 industry. 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. Following the PEAC meeting, the committee members provided additional recommendations on how to best communicate to patients about cybersecurity vulnerabilities. Additionally, a discussion paper entitled Communicating Cybersecurity Vulnerabilities to Patients: Considerations for a Framework was posted in October 2020 with an open docket for public comment. The feedback from all of these stakeholders is the foundation for this document.

The FDA is also co-leading the "Vulnerability Communications Task Group" (Healthcare and Public Health Sector, 2021) through the Healthcare and Public Health Sector Coordinating Council. The FDA expects that many of the outputs of the Task Group will further advance the maturity and capabilities of health care with respect to vulnerability communications, and interested stakeholders may wish to follow the Task Group's work.[1] Additionally, there are several relevant documents that may be helpful resources in framing the discussion elements in this paper (National Institute of Standards and Technology, 2018; National Telecommunications and Information Administration, 2016; Householder, 2019; U.S. Food and Drug Administration, 2016).

## Purpose

The *Best Practices for Communicating Cybersecurity Vulnerabilities to Patients* provides helpful information and elements for industry stakeholders, federal partners, and other interested stakeholders (hereafter referred to as "messengers") to consider when developing a cybersecurity communication strategy. These elements include:

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

[1] The outputs of the Vulnerability Communications Task Group will be available at: https://healthsectorcouncil.org/hscc-recommendations/

- outreach and distribution vehicles.

## Important Elements to Consider in the Communication Strategy

The feedback received at and following the 2019 PEAC Meeting (including that obtained through the FDA's Internal Message Testing Network) highlighted that certain elements are considered important to include in the development of safety communications for cybersecurity vulnerabilities. Such elements include assuring the interpretability of the message, clearly discussing risks and benefits, acknowledging and explaining the unknown, improving the availability and findability of the information. This document expounds on these elements, which 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, the messenger needs to communicate complex messages in clear and plain language consistent with the audience's need to receive and understand the messages 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 feasible, communicate with patients and caregivers as early as possible, especially if the cybersecurity vulnerability may present a risk to patient safety. 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. The FDA recognizes that messengers may not be able to communicate immediately upon learning of a vulnerability for numerous reasons. For example, time may be required to assess the nature of the vulnerability, what products are impacted, the possible severity of the vulnerability, and what mitigations are available. However, messengers, like the FDA, strive to communicate as quickly as possible, with the timeliness and frequency of communication tailored to the particular vulnerability and situation (U.S. Food and Drug

Administration, 2016). For instance, messengers may wish to communicate quickly when devices actively being exploited or where there is a credible threat that it will be exploited.[2]

Because the severity of cybersecurity vulnerabilities can change at any time (for example, the development of exploit code could increase the likelihood of exploitation), it is important for messengers to update vulnerability communications as needed to ensure that patients have access to the most up-to-date and relevant information. Given the evolving nature of vulnerabilities, it may help to explain what is known and unknown at the time of the communication. This is described in greater detail later in this document.

### 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 (that is, clear actions that patients and caregivers can take) that is easily accessible in the communication 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 take action to mitigate risks, as an update to their device may not yet exist, or they may need to wait for the medical device manufacturer, health care provider, or other party to take some action first. In these cases, communication materials that provide clear and concise instructions for recommended actions and focus on what patients and caregivers should do are important, including how they might identify if their device has been affected. If no action is recommended, communications that clearly state this fact help to mitigate against the perception of it being an oversight.

In some cases, messengers may recommend temporary actions to reduce risk exposure while more permanent or complete updates are developed and deployed. For both permanent and temporary solutions, messengers can clarify for patients whether the recommended actions are partially or fully addressing the risk. By being transparent in their communications, messengers can better manage patient expectations.

One way to help ensure communications are relevant, interpretable, and usable is to conduct message testing with target audiences. Organizations may want to consider having patient advisory boards and

[2] For additional discussion related to timeliness and frequency of communications, see the FDA's Guidance on Postmarket Management of Cybersecurity in Medical Devices and the CERT/CC CVD Guide, https://vuls.cert.org/confluence/display/CVD ("CERT/CC CVD Guide").

cybersecurity subject matter experts assist with message refinement to help ensure the message is both patient-friendly and technically accurate.

### Keep it Simple

To best reach the target audience, it is helpful to communicate about cybersecurity vulnerabilities in the simplest way possible. Using terminology that the target audience understands is a best practice in communications, and pilot testing the communication with the intended audience can help better assess what they do and do not understand (Centers for Disease Control and Prevention, 2019). Even when using simple terminology, audiences with low health literacy may struggle with certain concepts (U.S. Food and Drug Administration, 2013), so testing the communication can help ensure it is appropriate for the target audience. 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 for the name of a device. It could help patients if the communications clearly explain the difference between the name of the vulnerability and any affected medical devices.

In addition to using plain language, communicating any known numbers in a way that is easily understandable to different audiences (considering potential numeracy issues) can facilitate patient understanding (Fischoff, 2011).

As a matter of industry practice, cybersecurity vulnerabilities are often "scored" based on widely accepted rubrics such as the Common Vulnerability Scoring System (CVSS).[3] However, CVSS and other similar rubrics were not designed to capture patient-safety specific risks like those potentially introduced by medical device cybersecurity vulnerabilities. As a result, if messengers choose to communicate a numeric score like a CVSS score, then additional information could help patients and caregivers understand what the score may mean in the context of medical device safety. The FDA has qualified a tool, known as the "Rubric for Applying CVSS to Medical Devices," as a Medical Device Development Tool (MDDT) that messengers may voluntarily choose to use to assist with this process (Chase & Christey Coley, 2020).

[3] CVSS is currently maintained by the Forum of Incident Reponse and Security Team's (FIRST). See: https://www.first.org/.

### Keep it Readable for Diverse Audiences

While keeping it simple will help enable all audiences to better understand the communication, it is also helpful when 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 Latinx patients who may primarily speak Spanish, it may help reach the target audience if the safety communication is 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 complexity 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.

To enable availability of messages to a broad patient population, messengers may wish to put in place a process to make accurate cybersecurity vulnerability advisory translations in multiple languages available in a timely fashion. If there is a potential delay of the translated content, messengers may want to state in their advisories that translations will be forthcoming, as appropriate. Of note, it is a best practice to have those statements available not only in English but made available in the languages for which the translations are going to be available.

## 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, a careful discussion of both the risks and benefits of actions related to addressing the specific vulnerability can facilitate decision making. The goal is to help provide patients and caregivers with adequate 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, messengers could 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 identified in a device, but there are 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 and explain the reason for why this is unknown (i.e., due to limited detection capabilities).

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

The FDA and industry often communicate about medical device cybersecurity vulnerabilities. A communication about cybersecurity risks in medical devices that is easy to find is most likely to reach patients and caregivers. The elements below expound upon the best practices of availability and findability.

### 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 aids patient and public understanding and identification.

In addition, links to relevant resources could make it easier for patients to access important information and stay updated on the status of the vulnerability. Where relevant and appropriate, consider including links to additional relevant sources that may have more information, such as a manufacturer, the Health Sector Cybersecurity Coordinating Center (HC3), or the Cybersecurity Infrastructure Security Advisory (CISA) website. Additionally, where appropriate, including contact information and resources to report issues can enable the patients' voice to be heard. For example, the MedWatch website is an important resource where patients can report harm or issues with their devices to the FDA.

### 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, 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 fundamental to safety communication structure. To help patients and caregivers quickly find information relevant to them, safety communications that lead with the main message and recommendations for patients and caregivers are most effective.

Good organization also helps when constructing safety communications. This can include considering the audience and putting clear and succinct messages that are most relevant to patients and caregivers at the top, near the beginning of the safety communication (Peters, Dieckmann, Dixon, Hibbard, & Mertz, 2007; Plain Language.gov. , 2011). The FDA's Internal Message Testing Network also showed a preference for communications that are short. Including information about specific diseases or affected medical devices, as applicable, at the top of the communication is also helpful.

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 (Lorch & Lorch, 1995; Trevena, 2006). 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 wish to conduct outreach with partner organizations to help inform the target audience. Different types of vulnerabilities and audiences may benefit from different approaches, so it helps to consider which combination of distribution vehicles could be used to maximize outreach.

### Outreach Plan

An outreach plan includes consideration of 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 another consideration, 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. Outreach partners may include, but are not limited to, patient organizations, community groups, research partners, federal agencies, and advisory boards. This planning may help create a network that can facilitate, when the time comes, rapid communication deployment. For example, collaborations and partnerships with minority health professional organizations can serve a key role in supporting effective communication and outreach, and may be able to help with access and even translation (U.S. Food and Drug Administration, 2013). Creating a template for these types of communications may also enable faster communications. There may be situations where the messenger may not be able to reach the end user for many reasons. However, using communication vehicles that best match the circumstance and needs of the target audience may increase the likelihood that messengers will be able to reach the end user.

## Distribution Vehicles

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 Latinx population, then the distribution vehicles may be augmented to assure outreach to these populations. Just as language may be tailored for the target audience, distribution vehicles may also be tailored for the target audience.

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 of 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 the 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.[4]

- **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). Messengers may want to communicate through social media based on their target audience, although it may be advantageous to diversify communication vehicles and not rely on social media alone. Messengers may also want to consider the potential risks of disinformation spreading when drafting communications intended for social media platforms.
- **Television** – Participants also considered television to be a reliable source of information. Local television news could be an impactful medium for sharing health information, and earned media can be an affordable means to communicate. Organizations could consider whether this is an appropriate and feasible vehicle for them.
- **Websites** – Messengers use their own websites to disseminate safety information. Whether organizations use safety alerts or other media vehicles (such as a press release), 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.

Communication vehicles can be tailored to the specific population affected. For instance, while not mentioned by participants, radio may be a distribution vehicle to consider for reaching some populations (Seidenberg AB, 2017).

## 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

[4] Note that text messaging from messengers could contribute to an atmosphere for an effective phishing attack. It may be best to include some warning not to share personal information by text, so that patients do not get conditioned to share personal information if a scammer later reaches out asking for personal information.

severe, and more clinically impactful (U.S. Food & Drug Administration, 2018), it is increasingly important for the FDA, industry, and other messengers to consider ways to improve on cybersecurity safety communications. These best practices can help to advance this improvement.

Patients and caregivers prefer that communications be available, easy to find, and easy to understand. Additional considerations are that communications be timely, relevant, simple, and readable for a diverse audience, discuss the risks and benefits, and acknowledge any unknown information. Sharing information about cybersecurity vulnerabilities with patients and caregivers helps them make informed decisions about their health and their medical devices.

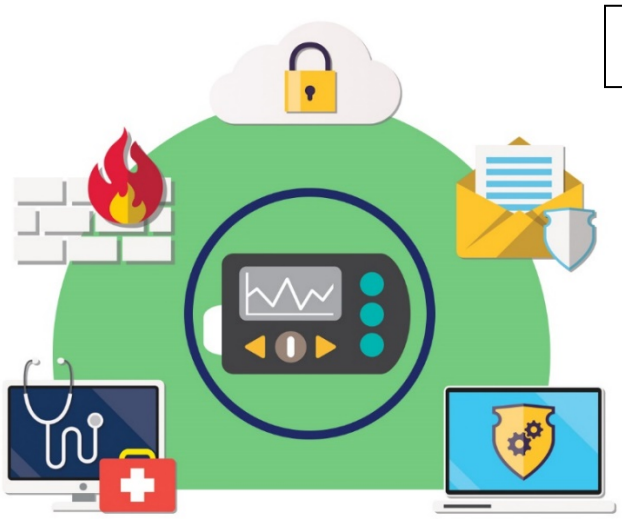
## Appendix: Sample Cybersecurity Vulnerability Safety Communication

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 risks, potentially impacting the safety and effectiveness of the device. These are **cybersecurity risks**.*

**Content current as of:**
Month/Day/Year



Español | 简体中文 | 한국어 | Tagalog | Việt

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**."

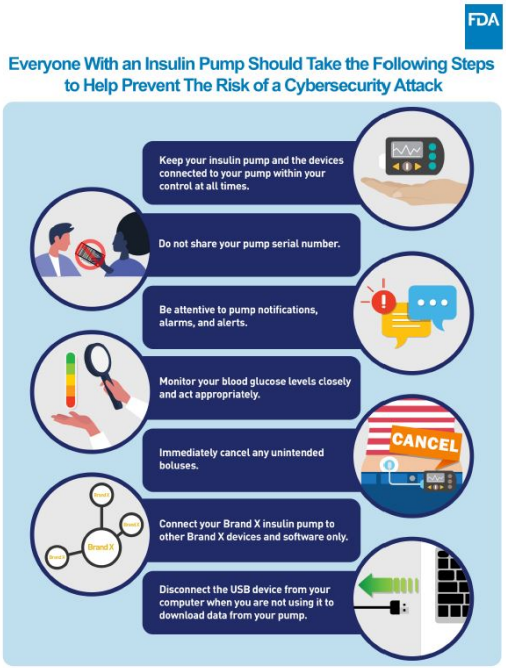
## Get Medical Help Right Away if You:

- 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
- Department of Homeland Security Cybersecurity Infrastructure Security Advisory (CISA)

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

Chase, M. P., & Christey Coley, S. M. (2020, October). *RUBRIC FOR APPLYING CVSS TO MEDICAL DEVICES*. Retrieved from MITRE Web Site: https://www.mitre.org/publications/technical-papers/rubric-for-applying-cvss-to-medical-devices

Cruz, T. B.-G. (2019). Pro-tobacco marketing and anti-tobacco campaigns aimed at vulnerable populations: A review of the literature. *Tobacco induced diseases*, 68.

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/

Fischoff, B. (2011). Chapter 7: Quantitative Information. In A. Fagerlin, & E. Peters, *Communicating Risks and Benefits: An Evidence-Based User's Guide* (pp. 53-61). Silver Spring: The Food and Drug Administration.

Healthcare and Public Health Sector. (2021). *HSCC Joint Cybersecurity Working Group Task Groups*. Retrieved June 1, 2021, from https://healthsectorcouncil.org/task-groups/

Householder, A. (2019, December 12). *The CERT Guide to Coordinated Vulnerability Disclosure*. Retrieved from https://vuls.cert.org/confluence/display/CVD

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

Lorch, R., & Lorch, E. (1995). Effects of organizational signals on text-processing strategies. *Journal of Educational Psychology*, 537-544.

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/

National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity.* Gaithersburg: National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

National Telecommunications and Information Administration. (2016, December 15). *Multistakeholder Process: Cybersecurity Vulnerabilities*. Retrieved from National Telecommunications and

Information Administration Web Site: https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities

Peters, E., Dieckmann, N., Dixon, A., Hibbard, J. H., & Mertz, C. K. (2007). Less is more in presenting quality information to consumers. *Medical Care Research and Review*, 169-90.

*Plain Language.gov.* . (2011, March). Retrieved from Federal plain language guidelines: http://www.plainlanguage.gov/howto/guidelines/FederalPLGuidelines/TOC.cfmExternal

Seidenberg AB, J. C. (2017). A National Study of Social Media, Television, Radio, and Internet Usage of Adults by Sexual Orientation and Smoking Status: Implications for Campaign Design. *nternational Journal of Environmental Research and Public Health*, 450.

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

Trevena, L. D. (2006). A systematic review on communicating with patients about evidence. *Journal of Evaluation in Clinical Practice*, 13-23.

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

U.S. Food and Drug Administration. (2013). *FDA Report: Ensuring Access to Adequate Information on Medical Products for All.* Silver Spring: FDA.

U.S. Food and Drug Administration. (2016). *Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff.* Silver Spring: U.S. Food and Drug Administration. Retrieved from https://www.fda.gov/media/95862/download

U.S. Food and Drug Administration. (2020, October 13). *Patient Engagement Advisory Committee*. Retrieved from U.S. Food and Drug Administration Web Site: https://www.fda.gov/AdvisoryCommittees/CommitteesMeetingMaterials/PatientEngagementAdvisoryCommittee/default.htm

(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.