Journal of Diabetes Science and Technology
2019, Vol. 13(5) 817–820
© 2019 Diabetes Technology Society
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/1932296819865655
journals.sagepub.com/home/dst
SAGE

The First Recall of a Diabetes Device Because of Cybersecurity Risks

David Klonoff, MD, FACP, FRCP (Edin), Fellow AIMBE[1] and Julia Han, BA[1]

Keywords
cybersecurity, diabetes, Do-It-Yourself (DIY), FDA, insulin pump, recall

Introduction

On June 27, 2019, the U.S. Food and Drug Administration (FDA) announced that they are warning patients and healthcare providers that certain Medtronic MiniMed insulin pumps are being recalled because of potential cybersecurity risks.[1] This is a historic decision because it represents the first time that a connected diabetes device has been voluntarily recalled by a manufacturer because of cybersecurity vulnerabilities. Prior to that date, FDA has issued device cybersecurity safety communications only for infusion pumps and implanted cardiac device along with their controllers.[2]

FDA recommended that patients replace affected Medtronic MiniMed pump models. In the United States, this means the 508 and the Paradigm pumps were affected, and in the other countries, yet other pumps were also affected. The warning applies to Medtronic insulin pumps that were introduced to the market before 2013.[3] The risk is that, because of cybersecurity vulnerabilities, a hacker could potentially connect wirelessly to a nearby Medtronic MiniMed insulin pump and change the pump's settings. In this case, control of the pump's settings could be wrested from the patient, caregiver, or healthcare provider and the result could be an insulin overdose[4] (resulting in hypoglycemia) or an insulin stoppage (resulting in ketoacidosis). The FDA announcement stated that FDA was not aware of any patients who may have been harmed by this particular cybersecurity vulnerability, but the risk of patient harm if such a vulnerability were left unaddressed is significant.

The Proposed Remedy

Medtronic, in a letter dated June 27, 2019 that was sent to patients and posted on its website, referred to this situation as being a safety notification.[5] Though not yet classified as a recall, the manufacturer's voluntary action to remove affected devices presently in use and replace with later generation insulin pumps that do not have this vulnerability is illustrative of its responsibility to protect the public health and well-being from products that present an uncontrolled risk of patient harm due to a cybersecurity vulnerability. In communicating to the public about this safety issue on June 27, 2019, Medtronic announced a program designed to give their out-of-warranty customers the option to exchange or upgrade their current legacy device.[6]

The company mentioned an eight-part plan for correcting the risk (see Table 1).[5] We agree with these recommendations. We think that Medtronic handled the situation correctly in voluntarily recalling their pumps because of a security flaw. We note that the 508 and Paradigm pumps come with a factory setting of a 10 U maximum bolus, but this default setting can be modified by the user to deliver a maximum bolus of 0 to 25 U.[7,8] We recommend that the maximum bolus dose in these pumps should be set at a safe amount to be selected by the user's physician, which will make it more difficult for a hacker to deliver a massive bolus of insulin all at one time.

Explaining a Recall to Patients

A worthy goal for healthcare professionals attempting to explain this recall to patients affected with diabetes is to balance reassuring their patients that this vulnerability would require considerable skill by a hacker and that, as patients, they can take extra precautions to make it more difficult for such a hack to occur, with urging vigilance and partaking of manufacturer-recommended remedies related to taking their product offline to make it less vulnerable but necessarily less convenient to use. The FDA announcement prudently stated, "it's important to remember that the increased use of wireless technology and software in medical devices can also offer safer, more convenient, and timely health care delivery."[1] At the same time, as medical devices are becoming more connected through wireless communication channels, they are

[1]Diabetes Research Institute, Mills-Peninsula Medical Center, San Mateo, CA, USA

Corresponding Author:
David C. Klonoff, MD, FACP, FRCP (Edin), Fellow AIMBE, Diabetes Research Institute, Mills-Peninsula Medical Center, 100 South San Mateo Drive, Room 5147, San Mateo, CA 94401, USA.
Email: dklonoff@diabetestechnology.org

Table 1. Cybersecurity Precautions Recommended for All Patients Using a MiniMed 508 Insulin Pump or a MiniMed Paradigm Series Insulin Pump in a Letter From Medtronic on June 27, 2019.[5]

- Keep your insulin pump and the devices that are 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
- Immediately cancel any unintended boluses
- Monitor your blood glucose levels closely and act as appropriate
- Do not connect to any third-party devices or use any software not authorized by Medtronic
- Disconnect your CareLink USB device from your computer when it is not being used to download data from your pump
- Get medical help right away if you experience symptoms of severe hypoglycemia or diabetic ketoacidosis, or suspect that your insulin pump settings or insulin delivery changed unexpectedly

simultaneously at greater risk of their information flow being diverted, altered, or shut off through cybersecurity breaches.

FDA will be convening a Patient Engagement Advisory Committee (PEAC) meeting[9] on September 10, 2019 about the cybersecurity of medical devices. The meeting will focus on how FDA, industry, and healthcare providers should communicate cybersecurity risks, as well as what patients want to know, and how they wish to receive this information.[10]

The precarious situation of attempting to balance greater opportunities for wireless communication with greater safety in the diabetes patient community (compared to patients who use devices for other diagnoses) can be challenging when device manufacturers interact with the Do-It-Yourself (DIY) community. The DIYers have depended on vulnerabilities in older insulin pumps like the ones in this story to hack into remotely controlled pumps and reprogram them with homebrewed software whose functions are not as yet available with FDA-cleared products. Patients with other diseases who use implanted or wearable wirelessly controlled devices have not been known to assume control over their own devices the way the diabetes DIY community has, which makes the challenge to find this balance more difficult for diabetes devices than for devices used for the other diseases.

Do-It-Yourself Products

Tidepool has announced a plan to leverage the FDA's interoperability plans[11] and submit a version of the DIY popular "Loop" App for automated insulin delivery called "Tidepool Loop."[12] Last year, Tidepool announced a collaboration with Insulet[13] and this year Tidepool announced a second collaboration with Medtronic.[14] If Tidepool Loop can gain FDA clearance, then DIY patients will be able to run this cleared closed loop software on modern pumps supported by these two manufacturers. Furthermore, these patients will have much less reason to want to use old unsupported pumps like the ones that are now being recalled.

On May 17, 2019, FDA took its most forceful position yet specifically against the use of DIY products by issuing a safety communication warning recommending against the use of unauthorized devices for diabetes management.[15] These include the types of devices that are currently used by the DIY community. This announcement came after the agency had received a report of a serious adverse event in which a patient's use of an unauthorized continuous glucose monitoring system along with an unauthorized automated insulin dosing (AID) system resulted in an insulin overdose requiring medical attention.[15]

This specific warning was probably not going to cause the DIY community to return to using only FDA-cleared products for their diabetes. However, the statement was important to show this community that what they are doing could be dangerous (not only from a risk of a security breach but also from bad code or malfunctioning hardware) and can result in an unintended insulin overdose. FDA cannot compel a patient to give up a device and accept a replacement in its stead when an identified cybersecurity vulnerability has been assessed as posing an "uncontrolled risk of patient harm." Nonetheless, manufacturers are strongly encouraged to make every good faith attempt to offer more secure products. If Tidepool Loop can gain FDA clearance, then there will likely be a rapid migration toward pumps that are compatible with this DIY software and the FDA's warning against DIY Products will finally be widely heeded.

An Earlier Insulin Pump Cybersecurity Issue

In 2016, the Animas OneTouch Ping was shown to have a security flaw.[16] We think that Animas handled the situation well through a coordinated vulnerability disclosure with a cybersecurity company. Animas recommended (1) disconnecting the pump's remote-control capability; (2) programming an upper limit to the amount of bolus insulin that can be delivered; (3) enabling a vibrating alarm to warn of an unauthorized insulin bolus; and (4) checking the pump's dosing log regularly to make sure no extra unaccounted-for insulin has been delivered.

The Significance of the Recall

The Medtronic recall announcement, released in conjunction with the FDA announcement, unlike the Animas announcement three years ago, did not mention a coordinated disclosure with a security firm. However, it has been well known in the DIY community and the cybersecurity community that the Medtronic pumps mentioned in the FDA recall announcement, as well as other types of older wireless medical devices that were developed before there was much general awareness of the significance of cybersecurity, contain a cybersecurity vulnerability. It is this vulnerability that allows most of the DIY systems to function. We believe that the FDA interoperability vision for AID systems[11] will result in more choice options for closed loop systems and spur innovation that will benefit the diabetes community. Other closed loop software might also be in the pipeline[17] to offer closed loop patients even additional choices.

Where Do We Go From Here?

Four stakeholders might be particularly affected by this recall. First, patients who are currently using an affected Medtronic MiniMed insulin pump can read instructions on how to adjust their pump settings in a letter from Medtronic (per Table 1) and what to discuss with their healthcare provider about upgrading to a newer safer model.[5] Second, healthcare professionals should a) read the safety communication released by the FDA about the potential cybersecurity risks of certain Medtronic MiniMed pumps[18] and b) discuss with their patients the safety issues of using a recalled pump and encourage their patients to follow the manufacturers' recommendations for safety.[5,6] Third, insulin pump manufacturers should carefully review the cybersecurity of their products already on the market and provide software patches or updates when possible. According to the FDA safety communication, Medtronic was not able to adequately update the MiniMed 508 and Paradigm insulin pumps with any new software or patch to address the devices' vulnerabilities.[18] For pumps being developed, we recommend that companies follow the DTSec Cybersecurity standard developed by Diabetes Technology Society in collaboration with FDA, other government agencies, industry, professional organizations, and independent experts in medicine, nursing, law, engineering, information technology, and standards.[19] This standard is the only consensus standard for diabetes device cybersecurity that contains both performance and assurance requirements. DTSec is currently in the process of being upgraded to become managed by a joint effort of the Institute of Electrical and Electronics Engineers (IEEE) and Underwriters Laboratories (UL). The FDA's draft guidance for Content of Premarket Submissions for Management of Cybersecurity in Medical Devices (released on October 18, 2018)[20] extends the agency's policies for cybersecurity beyond their original guidance on this topic (released on October 2, 2014).[21] The 2018 draft premarket cybersecurity guidance specifies that secure products require (1) trustworthy design, (2) submission of a cybersecurity bill of materials, (3) a capacity to accommodate patches or updates, and (4) adherence to specific labeling requirements. Fourth, FDA should be consistent in its efforts to protect the public and patients when marketed medical devices present cybersecurity concerns that can impact their safe performance.[22]

Conclusion

The recall of Medtronic pumps on June 27, 2019 might be the beginning of a new era in cybersecurity for diabetes devices. Hopefully, this historic event will lead patients, healthcare providers, device manufacturers, and the FDA, respectively, to redouble their efforts to insist on using, insist on prescribing, insist on manufacturing, and insist on requiring devices that meet established, sound security baselines in design and throughout the product's lifecycle.

Acknowledgment

The authors thank Annamarie Sucher for her expert editorial assistance.

Declaration of Conflicting Interests

The author(s) declared the following potential conflicts of interest with respect to the research, authorship, and/or publication of this article: DCK is a consultant to Abbott, EOFlow, Lifecare, Merck, Novo, and Voluntis. JH has nothing to disclose.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

1. U.S. Food and Drug Administration. FDA warns patients and health care providers about potential cybersecurity concerns with certain Medtronic insulin pumps. https://www.fda.gov/news-events/press-announcements/fda-warns-patients-and-health-care-providers-about-potential-cybersecurity-concerns-certain. Updated June 27, 2019. Accessed July 10, 2019.
2. U.S. Food and Drug Administration. Cybersecurity. https://www.fda.gov/medical-devices/digital-health/cybersecurity. Updated June 27, 2019. Accessed July 10, 2019.
3. Carlson J. Pre-2013 Medtronic insulin pumps could be vulnerable to hacking. http://www.startribune.com/pre-2013-medtronic-insulin-pumps-could-be-vulnerable-to-hacking/511906482/. Updated June 27, 2019. Accessed July 10, 2019.
4. Dameff CJ, Selzer JA, Fisher J, Killeen JP, Tully JL. Clinical cybersecurity training through novel high-fidelity simulations. *J Emerg Med*. 2019;56(2):233-238.
5. Dabbs J. MiniMed™ 508 insulin pump and MiniMed™ Paradigm™ series insulin pumps. https://www.medtronicdiabetes.com/customer-support/product-and-service-updates/notice11-letter. Accessed July 10, 2019.
6. Medtronic. Cybersecurity notice - legacy exchange program (US only). https://info.medtronicdiabetes.com/legacyexchange. Updated June 18, 2019. Accessed July 10, 2019.
7. Medtronic. Medtronic MiniMed user guide. https://www.medtronicdiabetes.com/sites/default/files/library/download-library/user-guides/508_user_guide.pdf. Accessed July 10, 2019.
8. Medtronic. The MiniMed paradigm 515 and 715 insulin pumps user guide, 2008. https://www.medtronicdiabetes.com/sites

/default/files/library/download-library/user-guides/x15_user_guide.pdf. Accessed July 10, 2019.

9. U.S. Food and Drug Administration. CDRH Patient Engagement Advisory Committee. https://www.fda.gov/about-fda/cdrh-patient-engagement/cdrh-patient-engagement-advisory-committee. Updated July 2, 2019. Accessed July 10, 2019.
10. U.S. Food and Drug Administration. Patient Engagement Advisory Committee; Notice of Meeting. https://s3.amazonaws.com/public-inspection.federalregister.gov/2019-14141.pdf. Updated July 2, 2019. Accessed July 10, 2019.
11. U.S. Food and Drug Administration. FDA authorizes first interoperable insulin pump intended to allow patients to customize treatment through their individual diabetes management devices. https://www.fda.gov/news-events/press-announcements/fda-authorizes-first-interoperable-insulin-pump-intended-allow-patients-customize-treatment-through. Updated February 14, 2019. Accessed July 10, 2019.
12. Look H. Tidepool intends to deliver Loop as a supported, FDA-regulated mobile app in the App Store. https://www.tidepool.org/blog/tidepool-delivering-loop. Updated October 9, 2018. Accessed July 10, 2019.
13. Motley Fool Transcription. Insulet Corporation (PODD) Q3 2018 Earnings Conference Call Transcript. https://www.fool.com/earnings/call-transcripts/2018/11/01/insulet-corporation-podd-q3-2018-earnings-conferen.aspx. Updated November 1, 2018 Accessed July 10, 2019.
14. Look H. Tidepool and Medtronic collaborate on Tidepool Loop in support of patient choice and interoperability. https://www.tidepool.org/blog/tidepool-loop-medtronic-collaboration. Updated June 7, 2019. Accessed July 10, 2019.
15. Food and Drug Administration. FDA Warns People with Diabetes and Health Care Providers Against the Use of Devices for Diabetes Management Not Authorized for Sale in the United States: FDA Safety Communication. https://www.fda.gov/medical-devices/safety-communications/fda-warns-people-diabetes-and-health-care-providers-against-use-devices-diabetes-management-not. Updated May 17, 2019. Accessed July 10, 2019.
16. Animas Corporation. Important Information about the cybersecurity of your OneTouch® Ping® Insulin Infusion Pump. https://www.animas.com/sites/animas.com/files/pdf/FINAL%20Letter%20to%20patients%20regarding%20OTP_10.04.16.16_WEB%20VERSION_0.PDF. Updated October 4, 2016. Accessed July 10, 2019.
17. Tandem Diabetes Care. About Tandem: Pipeline. https://www.tandemdiabetes.com/about-us/pipeline. Accessed July 10, 2019.
18. U.S. Food and Drug Administration. Certain Medtronic MiniMed Insulin Pumps Have Potential Cybersecurity Risks: FDA Safety Communication. https://www.fda.gov/medical-devices/safety-communications/certain-medtronic-minimed-insulin-pumps-have-potential-cybersecurity-risks-fda-safety-communication. Issued June 27, 2019. Updated July 1, 2019. Accessed July 10, 2019.
19. Diabetes Technology Society. Standard for wireless diabetes device security (DTSec). https://www.diabetestechnology.org/dtsec/DTSec%20Standard.pdf. Updated November 25, 2017. Accessed July 10, 2019.
20. U.S. Food and Drug Administration. Content of premarket submissions for management of cybersecurity in medical devices: guidance for industry and food and drug administration staff, October 2018. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices. Updated February 1, 2019. Accessed July 10, 2019.
21. U.S. Food and Drug Administration. Content of premarket submissions for management of cybersecurity in medical devices: guidance for industry and food and drug administration staff, October 2014. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices-0. Updated October 1, 2018. Accessed July 10, 2019.
22. U.S. Food and Drug Administration. Medical Device Safety Action Plan: Protecting Patients, Promoting Public Health. https://www.fda.gov/about-fda/cdrh-reports/medical-device-safety-action-plan-protecting-patients-promoting-public-health. Updated November 26, 2018. Accessed July 10, 2019.