Certain Medtronic MiniMed Insulin Pumps Have Potential Cybersecurity Risks: FDA Safety Communication

Date Issued: June 27, 2019

The FDA is warning patients and health care providers that certain Medtronic MiniMed™ insulin pumps have potential cybersecurity risks. Patients with diabetes using these models should switch their insulin pump to models that are better equipped to protect against these potential risks.

Medtronic is recalling the following affected MiniMed pumps and providing alternative insulin pumps to patients.

Pump Model	Software Version
MiniMed™ 508	All versions
MiniMed™ Paradigm™ 511	All versions
MiniMed™ Paradigm™ 512/712	All versions
MiniMed™ Paradigm™ 515/715	All versions
MiniMed™ Paradigm™ 522/722	All versions
MiniMed™ Paradigm™ 522K/722K	All versions
MiniMed™ Paradigm™ 523/723	Version 2.4A or lower
MiniMed™ Paradigm™ 523K/723K	Version 2.4A or lower
MiniMed™ Paradigm™ 712E*	All versions
MiniMed™ Paradigm™ Veo 554CM/754CM*	Version 2.7A or lower
MiniMed™ Paradigm™ Veo 554/754*	Version 2.6A or lower

* *Available outside the United States only*.

Important Recommendations for People who have Diabetes and their Caregivers

- Check to see if the model and software version of your insulin pump is affected. Read the Medtronic Patient Letter (https://www.medtronicdiabetes.com/customer-support/product-and-service-updates/notice11-letter) (http://www.fda.gov/about-fda/website-policies/website-disclaimer) to learn how to identify your pump's software version. If you live outside the United States, Medtronic will send you a notification letter with instructions based on the country where you live.

- Talk to your health care provider about a prescription to switch to a model with more cybersecurity protection.
- If you have questions about replacing your pump, call Medtronic at 1-866-222-2584 or go to Medtronic's website (https://info.medtronicdiabetes.com/legacyexchange) (http://www.fda.gov/about-fda/website-policies/website-disclaimer).

To minimize the potential risk of a cybersecurity attack while you are waiting for a replacement pump:

- Keep your insulin pump and the devices that are connected to your pump within your control at all times whenever possible.
- 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 Medtronic insulin pump to other Medtronic devices and software only.
- Disconnect the USB device from your computer when you are not using it to download data from your pump.

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.

Recommendations for Health Care Providers

Review the "Important Recommendations for People who have Diabetes and their Caregivers" section of this communication with patients who have affected devices.

Potential Cybersecurity Risks Associated with Certain Medtronic MiniMed Pumps

The FDA has become aware that an unauthorized person (someone other than a patient, patient caregiver, or health care provider) could potentially connect wirelessly to a nearby MiniMed insulin pump with cybersecurity vulnerabilities. This 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 and diabetic ketoacidosis.

Medtronic cannot update the MiniMed™ 508 and Paradigm™ insulin pump models to address these potential cybersecurity risks. As a result, the FDA recommends patients replace affected pumps with models that are better equipped to protect them from these risks. To date, the FDA is not aware of any reports of patient harm related to these potential cybersecurity risks.

For more information see:

- Department of Homeland Security Cybersecurity Infrastructure Security Advisory (https://www.us-cert.gov/ics/advisories/icsma-19-178-01)
- Medtronic Security Bulletin (https://www.medtronic.com/content/dam/medtronic-com/us-en/corporate/documents/Medtronic_Security_Bulletin_Diabetes_Paradigm_062719_FINAL.pdf) (http://www.fda.gov/about-fda/website-policies/website-disclaimer)

FDA Actions

The FDA has worked to assure Medtronic addresses this cybersecurity issue, including disclosing this information to the public and helping patients replace their affected insulin pump models with newer models. The FDA will keep the public informed if significant new information becomes available.

Reporting Problems with Your Device

If you think you have had a problem with your device, the FDA encourages you to report the problem through the MedWatch Voluntary Reporting Form (https://www.accessdata.fda.gov/scripts/medwatch/index.cfm?action=reporting.home).

Health care personnel employed by facilities that are subject to the FDA's user facility reporting requirements should follow the reporting procedures established by their facilities.

Questions?

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