

URGENT FIELD SAFETY NOTIFICATION

MiniMed™ 508 Insulin Pump and MiniMed™ Paradigm™ Series Insulin Pumps Cybersecurity Concerns

June 27, 2019

Dear Valued Customer:

You are receiving this letter because our records indicate you may be using a MiniMed™ 508 insulin pump or a MiniMed™ Paradigm™ series insulin pump. Because your safety is our top priority, we are making you aware of a potential cybersecurity risk.

Potential cybersecurity risk:

The MiniMed™ 508 insulin pump and the MiniMed™ Paradigm™ series insulin pumps are designed to communicate using a wireless radio frequency (RF) with other devices such as a blood glucose meters, glucose sensor transmitters, and CareLink™ USB devices.

Security researchers have identified potential cybersecurity vulnerabilities related to these insulin pumps. An unauthorized person with special technical skills and equipment could potentially connect wirelessly to a nearby insulin pump to change settings and control insulin delivery. This could lead to hypoglycemia (if additional insulin is delivered) or hyperglycemia and diabetic ketoacidosis (if not enough insulin is delivered).

IMPORTANT NOTE: At this time, we have received no confirmed reports of unauthorized persons changing settings or controlling insulin delivery.

ACTION REQUIRED:

For US Patients:

Due to this potential cybersecurity issue, we recommend that you speak with your healthcare provider about changing to a newer model insulin pump with increased cybersecurity protection, such as the MiniMed™ 670G insulin pump.

If you and your healthcare provider decide that updating to a newer insulin pump model is the right decision for you, please call Medtronic at 1-866-222-2584 or go to (<https://info.medtronicdiabetes.com/legacyexchange>) to explore your options and to begin the replacement process.

In the meantime, we recommend you take the cybersecurity precautions included below.

For Patients outside the US:

You will receive a notification letter with instructions based on the country you live in. We recommend that you speak with your healthcare provider to discuss the cybersecurity issue and the steps you can take to protect yourself. In the meantime, we recommend you take the cybersecurity precautions included below.

If you live in a country that does not have a newer model Medtronic insulin pump available to you, you should take the cybersecurity precautions included below to minimize the potential for a cybersecurity attack and to continue to take advantage of the benefits of insulin pump therapy.

CYBERSECURITY PRECAUTIONS RECOMMENDED FOR ALL PATIENTS

- 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

The following pump models ARE vulnerable to this potential issue:

Insulin Pump	Software Versions
MiniMed™ 508 pump	All
MiniMed™ Paradigm™ 511 pump	All
MiniMed™ Paradigm™ 512/712 pumps	All
MiniMed™ Paradigm™ 712E pump	All
MiniMed™ Paradigm™ 515/715 pumps	All
MiniMed™ Paradigm™ 522/722 pumps	All
MiniMed™ Paradigm™ 522K/722K pumps	All
MiniMed™ Paradigm™ 523/723 pumps	Software Versions 2.4A or lower
MiniMed™ Paradigm™ 523K/723K pumps	Software Versions 2.4A or lower
MiniMed™ Paradigm™ Veo™ 554/754 pumps	Software Versions 2.6A or lower
MiniMed™ Paradigm™ Veo™ 554CM/754CM pumps	Software Versions 2.7A or lower

To find the software version for the MiniMed™ Paradigm™ pumps, go to the **STATUS** screen:

- To open the **STATUS** screen, press **ESC** until the **STATUS** screen appears.
- To view more text on the **STATUS** screen, press the up or down arrow to scroll and view all the information.
- To exit the **STATUS** screen, press **ESC** until the **STATUS** screen disappears.

These pump models are **NOT** vulnerable to this issue:

Insulin Pump	Software Versions
MiniMed™ 620G pump	All
MiniMed™ 630G pump	All
MiniMed™ 640G pump	All
MiniMed™ 670G pump	All

You may also read the FDA's Safety Communication (<https://www.fda.gov/medical-devices/safety-communications/2019-safety-communications>) about this potential cybersecurity risk.

We apologize for any inconvenience this may cause. Your safety and satisfaction are our top priorities. We appreciate your time and attention in reading this important notification.

As always, we are here to support you. If you have further questions or need assistance, please call our 24-Hour Technical Support at: 1-800-646-4633.

Sincerely,



James Dabbs
Vice President, Quality Assurance
Medtronic Diabetes