IMPORTANT FIELD SAFETY NOTIFICATION

MiniMed™ Paradigm™ Series Insulin Pumps **Cybersecurity Concerns**

July 02, 2019

Dear Valued Customer:

You are receiving this letter because our records indicate you may be using a Medtronic MiniMed™ Paradigm™712, 715, 722 or 754 insulin pumps. Because your safety is our top priority, we are making you aware of a potential cybersecurity risk.

Potential cybersecurity risk:

The MiniMed™ Paradigm™ 712, 715, 722 or 754 insulin pumps are designed to communicate using a wireless radio frequency (RF) with other devices such as a blood glucose meter, glucose sensor transmitters, CareLink USB devices, and remote programmers.

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

IMPORTANT NOTE: We have received no reports of unauthorized people changing settings or controlling insulin delivery.

ACTION REQUIRED:

We recommend you take the following precautions to minimize the potential for a cybersecurity attack:

- 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

These pump models ARE vulnerable to this potential issue:

Insulin Pump
MiniMed™ Paradigm™ 712 pumps MiniMed™ Paradigm™ 715 pumps MiniMed™ Paradigm™ 722 pumps MiniMed™ Paradigm™ Veo™ 754 pumps with Software Versions 2.6A or lower

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

Insulin Pump
MiniMed™ Paradigm™ Veo /754 with Software Versions 2.7 or greater To find the software version for the MiniMed™ Paradigm™ Veo /754 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.
MiniMed™ 620G pump MiniMed™ 640G pump MiniMed™ 670G pump

Your safety and complete satisfaction are our top priorities. We are committed to delivering safe and effective therapies. 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 Helpline at: 1800-209-6777 from 9:30am to 9:30pm or Contact to your Immediate Medtronic person.

Sincerely

James Dabbs
Vice President, Quality Assurance
Medtronic Diabetes

FAQs

Q:

Why am I receiving this notice? >

A:

Medtronic takes customer safety and device security very seriously. Due to this potential cybersecurity issue, Medtronic is recommending customers speak with their healthcare provider (HCP) about changing to a newer model insulin pump.

Q:

Does my pump require replacement? >

A:

Due to this potential cybersecurity issue, Medtronic is recommending customers speak with their healthcare provider (HCP) about changing to a newer model insulin pump with increased cybersecurity protection, like the MiniMed™ 640G insulin pump.

In the meantime, we recommend you take the cybersecurity precautions to minimize the potential risks.

Q:

What is the cybersecurity concern? >

A:

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

Security researchers have identified potential cybersecurity vulnerabilities related to the communication protocol in 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).

Q:

How do I find the software version of my pump? >

A:

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.

Q:

What actions is Medtronic taking to address this cybersecurity concern? >

A:

We have notified the appropriate regulatory authorities, published an advisory about this potential security concern, and informed healthcare professionals and patients about precautionary steps that can be taken to protect the security of their pump.

Q:

My safety is important, what is Medtronic doing to anticipate security concerns and build-in safeguards to prevent them from happening? >

A:

As part of our commitment to customer safety and device security, Medtronic works closely with industry regulators and researchers to anticipate and respond to potential risks. In addition to our ongoing work with the security community, we have already made several important changes to enhance device security with our newer devices available in some countries today. We will continue to take steps to collaborate with industry researchers and regulators to improve device safety.

Q:

How and when will Medtronic fix this concern? >

A:

Medtronic takes customer safety and device security very seriously. We have already introduced a new generation of insulin pumps that is not affected by this issue.

Q:

Does this impact the MiniMed™ 600 series insulin pumps? How are the MiniMed™ 600 series insulin pumps different? >

A:

No. This vulnerability does not impact the MiniMed™ 600 series insulin pumps because they use encrypted communication which is completely different from the communication used by the Paradigm pump models.

The MiniMed™ 600 series insulin pumps include the MiniMed™ 630G and MiniMed™ 670G systems in the US and the MiniMed™ 620G and 640G systems outside of the US.

Q:

What do you recommend I do now to protect my insulin pump security? >

A:

If you feel concerned:

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.

Q:

Should I replace my pump with a new 600 series pump? >

A:

Every person with diabetes should make decisions about their insulin pump therapy along with their healthcare team. We recommend you talk about this with your healthcare team.