Central Drugs Standard Control Organization

Directorate General of Health Services
Ministry of Health and Family Welfare
Government of India
(Medical Devices and Diagnostics Division)
Email: ddcimd-cdsco@nic.in
Food & Drugs Administration Bhavan,
Kotla Road, New Delhi.

File No: 29/Misc/03/2019-DC (100) **Date: 2nd July 2019**

MEDICAL DEVICE ALERT

DEVICE

Minimed™ Paradigm™ (MMT-715, MMT-712 & MMT-722) and MiniMed™ Paradigm™ Veo™ (MMT-754) Insulin Pumps.

BACKGROUND

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.

US FDA issue safety alert on 27.06.2019 indicating the warning to the patients and healthcare providers that "Certain Medtronic MiniMed Insulin Pumps Have Potential Cybersecurity Risks".

PROBLEM

The MiniMed™ Paradigm™ series insulin pumps (MMT-715, MMT-712, MMT-722, MMT-754) 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 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.

ACTION BY

- Medical Directors/Healthcare professionals
- Distributors and the Users
- Staff involved in the management of patients.

ACTION

- Check to see if the model and software version of your insulin pump is affected.
- Talk to your health care provider about a prescription to switch to a model with more cybersecurity protection.
- 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.

ADVERSE EFFECTS

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.

These pump models ARE vulnerable to this potential issue:

Insulin Pump
MiniMed™ Paradigm™ 715 pumps MiniMed™ Paradigm™ 712 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

Important Note: CDSCO have not received any complaints from the market on this issue.

FURTHER DETAILS & CONTACTS

India Medtronic Pvt. Ltd. had issued a FIELD SAFETY NOTIFICATION on MiniMed™ Paradigm™ Series Insulin Pumps Cybersecurity Concerns on June 27, 2019 which is attached herewith this alert.

- India Medtronic Pvt. Ltd.,
  4th Floor, Tower A & B, SAS Tower,
  The Medicity Complex, Sec-38, Gurugram-122001
  Direct line: +91-0124-470 9800

Medtronic
18000 Devonshire St.
Northridge, CA 91325
www.medtronicdiabetes.com

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.

930M19927-011 12JUN2019 ©2019 Medtronic. All rights reserved. Medtronic, Medtronic logo and Further, Together are trademarks of Medtronic. All other brands are trademarks of a Medtronic company.

Medtronic
18000 Devonshire St.
Northridge, CA 91325
www.medtronicdiabetes.com

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

930M19927-011 12JUN2019 ©2019 Medtronic. All rights reserved. Medtronic, Medtronic logo and Further, Together are trademarks of Medtronic. All other brands are trademarks of a Medtronic company.

Medtronic
18000 Devonshire St.
Northridge, CA 91325
www.medtronicdiabetes.com

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

930M19927-011 12JUN2019 ©2019 Medtronic. All rights reserved. Medtronic, Medtronic logo and Further, Together are trademarks of Medtronic. All other brands are trademarks of a Medtronic company.