

URGENT FIELD SAFETY NOTIFICATION
MiniMed™ remote controller (MMT-500 or MMT-503)
Potential security issue

08 August 2018

Dear valued clinician:

Our records show that you or one of your patients may be using an optional MiniMed™ remote controller model number **MMT-500** or **MMT-503**.

Because patient safety is our top priority, we are informing you of a potential security risk related to the Medtronic MiniMed™ 508 and Medtronic MiniMed™ Paradigm™ series insulin pumps when using the corresponding MiniMed™ remote controller.





Explanation of the issue

The Medtronic remote controller, which uses a wireless (RF) radio frequency to communicate with the insulin pumps, helps in programming a set amount of insulin (or bolus) into a Medtronic pump discreetly while keeping the device concealed.

An external security researcher has identified a potential vulnerability related to the MiniMed™ Paradigm™ family of insulin pumps and corresponding remote controller. The researcher's report states that an unauthorized individual in close proximity of an insulin pump user could potentially copy the wireless radio frequency (RF) signals from the user's remote controller (while they are in the process of delivering a remote bolus) and play those back later to deliver an involuntary bolus of insulin to the user. This could lead to potential health risks such as hypoglycemia if additional insulin is delivered beyond the user's insulin requirements.

The following list shows the Medtronic remote controller and compatible Medtronic insulin pump(s) that are vulnerable to this issue.

| Remote controller | Model Number Location | Compatible Insulin pump(s) |
|-------------------|--------------------------|----------------------------|
|-------------------|--------------------------|----------------------------|

| | | |
|---|--|--|
|  <p>MiniMed™ remote controller</p> <p>MMT-500</p> |  <p>The model # is behind the remote under the barcode</p> | <p>Medtronic MiniMed™ 508 pump</p> |
|  <p>MiniMed™ remote controller</p> <p>MMT-503</p> |  <p>The model # is behind the remote under the barcode</p> | <p>MiniMed™ Paradigm™ 511 pump</p> <p>MiniMed™ Paradigm™ 512/712 pumps</p> <p>MiniMed™ Paradigm™ 515/715 pumps</p> <p>MiniMed™ Paradigm™ 522/722 pumps</p> <p>MiniMed™ Paradigm™ 523/723 pumps</p> <p>MiniMed™ Paradigm™ 523(K)/723(K) pumps</p> <p>MiniMed™ 530G 551/751 pumps</p> <p>MiniMed™ Paradigm™ Veo™ 554/754</p> |

Several factors must occur for your patient's pump to be vulnerable:

1. The remote option for the pump would need to be enabled. This is not a factory-delivered default, and a user must choose this option.
2. The user's remote controller ID needs to be registered to the pump.
3. The Easy Bolus™ option would need to be turned on and a bolus step size programmed in the pump.
4. An unauthorized individual would need to be in close proximity of the user, with necessary equipment to copy the RF signals activated, when the user is delivering a bolus using the remote controller.
5. The unauthorized individual would need to be in close proximity of the user to play back the RF signals to deliver a malicious remote bolus.
6. The user would need to ignore the pump alerts, which indicates that a remote bolus is being delivered.

Protecting the security of MiniMed™ insulin pumps

If you or your patients are concerned about this matter, the following are some precautions that can be taken to minimize risk to yourself and your patients:

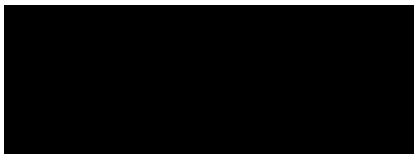
- Turning off Easy Bolus™ feature when not intending to use the remote bolus option
- Being attentive to the pump alerts, especially when the easy bolus option is turned on
- Avoiding any connection to third-party devices not authorized by Medtronic

Please note that if your patient has never programmed a remote controller ID into their pump and never programmed the Easy Bolus™ option, they are not susceptible to this vulnerability.

The MiniMed™ Paradigm™ family of insulin pumps remain safe and effective for diabetes management, so we encourage users to continue their therapy as they normally would and take these precautionary steps if concerned.

At Medtronic, patient safety is our top priority, and we are committed to delivering safe and effective therapies that undergo rigorous clinical, quality, manufacturing and regulatory controls to ensure this for our customers. We appreciate your time and attention in reading this important notification.

Sincerely,



Diana Teo
Quality Management System Manager
South East Asia
Medtronic

cc: The Chairman Medical Board and relevant Head of Departments



49 Changi South Avenue 2
Singapore 486056
www.medtronic.com

tel +65 6436 5000
fax +65 6776 6355

Field Action Customer Confirmation Form
MiniMed™ remote controller (MMT-500 or MMT-503)
Potential security issue

ALL CUSTOMERS PLEASE COMPLETE THE FORM IN ITS ENTIRETY

| Customer Contact Details | Medtronic Contact Details |
|---------------------------------|---------------------------|
| | Name: |
| Hospital / HCP/Customer: | Contact: |
| Address: | Email: |
| | |
| Phone no: | |
| E-mail: | |
| | |

| Product Code | Serial # of the affected unit |
|--------------|-------------------------------|
| | |

I have read and understand the instructions provided and taken and acknowledge receipt of the MiniMed™ remote controller (MMT-500 or MMT-503) Potential security issue notification dated 8 August 2018 by signing below:

Name: _____ (print) Signature: _____ Stamp: _____ Date: _____