Vulnerability Summary

External security researchers Billy Rios and Jonathan Butts from WhiteScope LLC have identified vulnerabilities in the Medtronic 9790 CareLink™ Programmer.

These vulnerabilities can allow an individual who has physical control of the programmer to access files that may contain Protected Health Information (PHI) or Personally Identifiable Information (PII). Further proactive internal review by Medtronic found similar vulnerabilities on the Medtronic 2090 CareLink Programmer and 29901 Encore™ Programmer.

Medtronic CareLink and Encore programmers are devices used by trained personnel at hospitals and clinics to program and manage Medtronic cardiac implantable electronic devices, such as pacemakers.

In general, PHI/PII is intended to be stored on the programmers for short periods of time before being transferred to other medical systems or printed to paper reports. If the PHI/PII settings are not properly managed or the programmer is not properly retired, patient PHI/PII may remain on a programmer longer than necessary. The specific types of PHI/PII stored by a programmer includes device serial number and device configuration settings. Other types of PHI/PII potentially stored on a programmer is determined by the personnel using the system.

Medtronic has worked with the healthcare organizations which have experienced the loss of 9790 and 2090 programmers to identify 38 patients whose data may have been exposed due to these vulnerabilities.

These vulnerabilities cannot be exploited remotely, meaning that to gain access to PHI or PII someone would need physical access to a programmer.
Mitigations
The CareLink 9790 Programmer was placed into end-of-life status in 2005 and is no longer supported by Medtronic. If a customer has a CareLink 9790 Programmer, they should return the programmer to Medtronic.

The CareLink 2090 and 29901 Encore programmers store PHI/PII as part of their normal operating procedures and should be handled, managed and secured in a manner consistent with the applicable laws for patient data privacy. The management and deletion of PHI/PII information on a programmer is under the control of the programmer user, in accordance with product labeling. PHI/PII should be retained on these programmers for the least amount of time necessary for its intended use.

Customers should refer to the programmer reference manual for instructions on setting the PHI/PII retention limit and deleting all PHI/PII prior to returning a retired programmer to Medtronic. Customers should contact their Medtronic representative for proper disposal and PHI/PII retention-setting assistance.

Additionally, Medtronic recommends that customers continue to follow the security guidance detailed in the CareLink 2090 programmer and CareLink Encore 29901 programmer reference manuals. This guidance includes maintaining good physical controls over the programmer and having a secure physical environment that prevents unauthorized access to the CareLink 2090 or CareLink Encore 29901 programmer. Customers should only use programmers obtained directly from Medtronic and should not use products provided or obtained by any third party.

Customers with questions or concerns about their programmers should contact Medtronic Technical Services at 800-638-1991.

Medtronic actively reviews its security practices to mitigate risks during pre-market development and post-market use. For more information on Medtronic’s product security efforts visit www.medtronic.com/security.

The complete updated advisory issued by ICS-CERT can be found here.