Security Update
Jan. 19, 2018

Background
Widely-publicized cybersecurity vulnerabilities known as Spectre and Meltdown, which take advantage of an optimization flaw impacting processors in nearly every computer and mobile device, were identified at the beginning of January 2018. This vulnerability could allow an attacker who is able to run arbitrary code on a computer to view data even though not authorized to do so. These vulnerabilities were shared from a number of sources, including the National Health Information Sharing and Analysis Center (NH-ISAC) and the United States Computer Emergency Readiness Team (US-CERT).

Medtronic Response
Medtronic is aware of the issue and understands that it may impact manufacturers and products differently. Our technical teams are currently analyzing the situation to better understand any potential impact to our products, as well as our enterprise environment. At this time, no evidence suggests that Medtronic products are directly impacted by the Spectre/Meltdown vulnerabilities. At Medtronic, we take cybersecurity matters seriously and have teams engaged in these matters on a continual basis.

Recommendations
As part of our comprehensive information security program, we may release future updates to products to further reduce the risk associated with these vulnerabilities.

For users of Medtronic applications on their own systems and mobile devices, please apply your manufacturer-recommended updates.

For More Information
US CERT has created a vulnerability note which provides additional information related to Meltdown and Spectre.
US-CERT Notice: Vulnerability Note VU#584653