TOSHIBA MEDICAL

Made For life

WannaCry Ransomware
(AKA WannaCrypt, WannaCrypt0r, Wanna Decryptor)

Medical imaging safety goes beyond radiation dose and extends to other areas, including cyber threats like the WannaCry Ransomware. Toshiba America Medical Systems, Inc. takes these security vulnerabilities very seriously. In fact, Toshiba America Medical Systems was the first manufacturer to meet the U.S. Department of Defense's strict security guidelines and receive Authority to Operate (ATO) for CT, and now has ATO across all modalities.

By receiving ATO status, Toshiba America Medical Systems has met the Air Force and Defense Health Agency's (DHA) guidelines for ensuring protection of Patient Health Information (PHI) and guarding against malware, viruses and malicious software.

Cyber threats may present a significant risk to healthcare providers' and patients' data. Toshiba America Medical Systems understands these risks and works diligently to assist our customers with protection of this data, including different security solutions to thwart and protect against attacks like the recent WannaCry Ransomware. Some of these offerings can be viewed on our website here.

However, when systems are connected to networks with Internet access, the PCs (including Toshiba products) incorporated in them can become susceptible to malicious software attacks. Therefore all customers must ensure that adequate security measures have been implemented into their network.

Customers with security questions or concerns can email TAMS-Security@tams.com.
24x7 customer support is available at (800) 521-1968.