Network Security Policy

Canon Medical Systems USA, Inc. takes protection of PHI, PII, and security of Canon Medical Systems devices very seriously.

With the release of Ransomware and other malicious attacks that has crippled many healthcare facilities across the globe, Canon Medical Systems is committed to providing our customers with certain security solutions to minimize any security vulnerabilities.

In keeping with the widespread advancement of Information Technology (IT) within the medical imaging industry, Canon Medical Systems recognizes the importance of cyber security and protection of Patient Health Information (PHI). Canon Medical Systems offers the latest in medical imaging equipment, incorporating flexible information management and real-time sharing via networks, including integration with Radiology Information Systems (RIS) and Picture Archiving and Communication Systems (PACS). With this integrated connectivity, Canon Medical Systems recognizes the importance of providing our customers with secure medical equipment to protect patient information, and to provide available malware and virus control.

However, when systems are connected to networks with Internet access, the Operating System , including Canon Medical Systems diagnostic equipment, incorporated in them can become susceptible to unauthorized access which leads to software attacks. Therefore all customers must ensure that adequate security measures have been implemented into their network. As described in the FDA Post-Market Cybersecurity Guidance3, Cybersecurity risk management is a shared responsibility and no stakeholder can guarantee 100 percent protection. Canon Medical Systems therefore strongly recommends that the customer's network environment provide the necessary network security measures, including access-control mechanisms, firewalls, Intrusion Detection Systems (IDSs) and user procedures and training to adequately protect critical medical imaging systems from unauthorized access and thus keep them secure and performing at optimum levels.

Canon Medical Systems approach to supporting its customers in addressing security threats such as RansomWare, viruses, malware, and malicious attacks, is as follows.

- All currently manufactured Canon Medical Systems Corporation diagnostic image making devices incorporate McAfee® Solidifier, a whitelist antivirus software.[1] This centrally managed whitelisting solution uses a dynamic trust model and innovative security features that thwart advanced persistent threats — without requiring signature updates or labor-intensive list management.[2]
- All currently manufactured Canon Medical Systems Corporation medical imaging systems incorporate Windows 7.
- Selected Canon Medical Systems Corporation medical imaging systems have the option for advanced security that follows the federal government strict security guidelines of Risk Management Framework (RMF).
- Only authorized Canon Medical Systems personnel or Canon Medical Systems trained technicians are allowed to install factory released software under Canon Medical Systems warranty or contract.
- After validation, Canon Medical Systems Corporation provides software updates from Microsoft® and other applicable companies to control security threats.
- Canon Medical Systems Corporation validates all medical imaging system software, including software patches, prior to installation ensuring safe and reliable performance. Canon Medical Systems Corporation delivers all of its new products to customers free of infections or malware as of the date of delivery.
- Canon Medical Systems offers a Cybersecurity-checking and restoration service for Canon Medical Systems diagnostic imaging systems that have been infected or compromised. A fee is charged for both these services. Canon Medical Systems customer engineers are able to run a virus check using their provided service tools. If a Cybersecurity threat is discovered, Canon Medical Systems will reload the operating system and application software and restore it to the original condition.
- Unauthorized installation of any commercially available antivirus, 3rd party software, or software not validated by Canon Medical Systems in the medical imaging system voids the product warranty. Furthermore, Canon Medical Systems will not be responsible for loss, contamination of patient data, or any performance issues caused by such installation.

Canon Medical Systems eProtect Authentication and Malware Protection Device

eProtect is the quickest, simplest and most secure protection for Canon Medical Systems equipment. eProtect is a specially configured network device designed to isolate Canon Medical Systems diagnostic products from hospital network traffic by incorporating network segmentation.

eProtect will control and limit traffic into and out of Canon Medical Systems products to allow DICOM services such as modality worklist, storage to PACS and workstations, structured reports and query & retrieve. At the same time, eProtect restricts unnecessary network traffic from reaching the medical device. This unnecessary network traffic, however is not limited to Ransomware, viruses, malware and malicious attacks.

Canon Medical Systems has found this to be the best form of malware protection for Canon Medical Systems medical imaging equipment. eProtect is provided free of charge to Canon Medical Systems warranty and contract customers.

InnerVision with Remote Connectivity Suite

InnerVision is Canon Medical Systems "Remote Support and Diagnostics" suite. InnerVision is a networking technology set up to allow remote service and support via VPN connections to our installed base of medical imaging systems.

Designed along industry standard security guidelines, InnerVision can set up discrete VPN tunnels for each medical imaging device. Canon Medical Systems support engineers, In-Touch application specialists, and customer engineers may then connect through those secure VPN tunnels to assess, troubleshoot and service issues and application support.

A VPN (Virtual Private Network) is the secure network connection from the customer's site to Canon Medical Systems HQ. It is the backbone through which InnerVision services operate.

A VPN connection is referred to as a "tunnel". There are various methods of establishing these tunnels. There are two VPN methods (protocols) used by Canon Medical Systems depending on the overall setup at the customer's site:

- IPSec (IP Security)
- SSL (Secure Socket Layer)

CANON MEDICAL SYSTEMS USA, INC.
2441 Michelle Drive, Tustin CA 92780 | 800.421.1968

With InnerVision SP-Firewall or TVR configuration will control and limit traffic into and out of Canon Medical Systems Corporation products to allow DICOM services such as modality worklist, storage to PACS and workstations, structured reports and query & retrieve. At the same time, InnerVision SP-Firewall and TVR configuration will restrict unnecessary network traffic from reaching the medical device by incorporating network segmentation. This unnecessary network traffic, however is not limited to Ransomware, viruses, malware and malicious attacks.

Contact Canon Medical Systems Security
Please email CanonMedicalSystemsSecurity@us.medical.canon with any questions or concerns.

24/7 Support: (800) 521-1968

Security Advisories and Supplemental Information

- For a detailed list of products and security implementations, **click here**
- WannaCry, **click here**
- CPU Hardware vulnerable to side-channel attacks, AKA Meltdown and Spectre, **click here**
- Key Reinstallation Attacks, AKA Krack, **click here**
- MicroTik Winbox Vulnerability **click here**
- Kwampirs Trojan propagated by Orangeworm, **click here**

[1] Excludes CXDI, Radrex, Harmony, Viamo, and Artida products.

[2] http://www.mcafee.com/us/products/application-control.aspx

[3] https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm482022.pdf

V1.2K

CANON MEDICAL SYSTEMS USA, INC.
2441 Michelle Drive, Tustin CA 92780 | 800.421.1968

Made For life