Canon

Canon Medical Systems USA, Inc.

Security Network 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[1] across the globe, Canon Medical Systems is committed to providing our customers with security solutions to minimize security vulnerabilities and the threat vector thereby significantly lowering the risk to your Canon Medical Systems imaging device.

In keeping with the widespread advancement of Information Technology (IT) within the medical imaging industry, Canon Medical Systems recognizes the importance of Cybersecurity 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 malware and virus control.

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 Guidance[2], the Healthcare and Public Health Sector Coordinating Council (HSCC) Joint Security Plan (JSP)[3], and the Global Diagnostic Imaging Healthcare IT & Radiation Therapy Trade Association (DITTA) White Paper on Cybersecurity[4], 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. For further information, visit our corporate Product Security Policy.

Canon Medical Systems practices Cybersecurity Best Practices. In doing so, 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[5] incorporate McAfee® Solidifier[6] or Microsoft AppLocker[7], a whitelist antivirus software. 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[5].

- All currently manufactured Canon Medical Systems Corporation medical imaging systems incorporate currently manufactured and supported Windows OS.

- 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 service agreement.

- After validation, Canon Medical Systems Corporation provides software updates from Microsoft® and other applicable companies to control security threats. Visit our OS and 3rd party patching policy for further information.

- 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 offers a second layer of Cybersecurity protection through Gateway Gold or Gateway Platinum. These firewall appliances provide a Whitelist deny-all firewall protection while segmenting the system for all fixed imaging devices. These firewall appliances provide significant reduction to risk by minimizing the threat vector of the imaging device.

- Canon Medical Systems offers InnerVison for UL through a secure HTTPSon-demand, connection for application and service support.

- Canon Medical Systems provides a dedicated Global Product Security Incident Response Team (PSIRT) for Security Incident Response . This service is available to all of our customers 24x7 to report any questions, concerns, or issues regarding vulnerabilities or threats.

- Canon Medical Systems provides public posting of Security Advisories as recommended by the HSCC JSP both on the Canon Medical Systems public webpage and the Department of Homeland Security ICS-CERT Division (when applicable)

- Canon Medical Systems provides at no cost all released OS and 3rd party updates to the applicable systems

- Canon Medical Systems provides a detailed overview of the Cybersecurity protection for your currently installed Canon Medical Systems device to easily determine the protection provided or offered.

Note: Canon UL SSL VPN Technical Summary.pdf

Contact Canon Medical Systems security
Email: CybersecurityRiskManagement@us.medical.canon
24/7 Support: (800) 521-1968

[1] https://www.theverge.com/2019/4/4/18293817/cybersecurity-hospitals-health-care-scan-simulation
https://securityboulevard.com/2019/02/cyber-a ttack-costs-can-cripple-small-and-medium-sized-businesses/
http://theconversation.com/why-has-healthcare-become-such-a-target-for-cyber-attackers-80656
[2] https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm482022.pdf
[3] https://healthsectorcouncil.org/wp-content/uploads/2019/01/HSCC-MEDTECH-JSP-v1.pdf
[4] https://www.globalditta.org/uploads/media/DITTA_White_paper_on_Cybersecurity_-_Feb._2019_-_Final.pdf
[5] For FM, Omnera, URS, and Digital Upgrade Room Kits for X-Ray portables and floor mounted systems allow McAfee AV to be installed and managed by the facility. McAfee Embedded Control is not installed.
[6] https://www.mcafee.com/enterprise/en-us/products/embedded-control.html
[7] All Windows 10 Ultrasound systems has AppLocker standard and McAfee Solidifier as an option. All other products come standard with McAfee Solidifier

V1.5

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

Made For life