Manufacturer Disclosure Statement for Medical Device Security -- MDS2

Carestream Health, Inc ImageView V1.7 AJ8791 27-Sep-2020

Question ID	Question		See note
DOC-1	Manufacturer Name	Carestream Health, Inc.	__
DOC-2	Device Description	X-Ray Imaging Systems	__
DOC-3	Device Model	ImageView V1.7	__
DOC-4	Document ID	AJ8791	__
DOC-5	Manufacturer Contact Information	1-800-328-2910 health.imaging.tsc@carestreamhealth.com	__
DOC-6	Intended use of device in network-connected environment:	X-Ray Imaging System	__
DOC-7	Document Release Date	9/27/2020	__
DOC-8	Coordinated Vulnerability Disclosure: Does the manufacturer have a vulnerability disclosure program for this device?	Yes	__
DOC-9	ISAO: Is the manufacturer part of an Information Sharing and Analysis Organization?	Yes	__
DOC-10	Diagram: Is a network or data flow diagram available that indicates connections to other system components or expected external resources?	Yes	__
DOC-11	SaMD: Is the device Software as a Medical Device (i.e. software-only, no hardware)?	No	__
DOC-11.1	Does the SaMD contain an operating system?	N/A	__
DOC-11.2	Does the SaMD rely on an owner/operator provided operating system?	N/A	__
DOC-11.3	Is the SaMD hosted by the manufacturer?	N/A	
DOC-11.4	Is the SaMD hosted by the customer?	N/A	__
	MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION		
MPII-1	Can this device display, transmit, store, or modify personally identifiable information (e.g. electronic Protected Health Information (ePHI))?	Yes	__
MPII-2	Does the device maintain personally identifiable information?	Yes	
MPII-2.1	Does the device maintain personally identifiable information temporarily in volatile memory (i.e., until cleared by power-off or reset)?	Yes	__
MPII-2.2	Does the device store personally identifiable information persistently on internal media?	Yes	__
MPII-2.3	Is personally identifiable information preserved in the device's non-volatile memory until explicitly erased?	Yes	__
MPII-2.4	Does the device store personally identifiable information in a database?	Yes	__
MPII-2.5	Does the device allow configuration to automatically delete local personally identifiable information after it is stored to a long term solution?	Yes	__
MPII-2.6	Does the device import/export personally identifiable information with other systems (e.g., a wearable monitoring device might export personally identifiable information to a server)?	Yes	__
MPII-2.7	Does the device maintain personally identifiable information when powered off, or during power service interruptions?	Yes	__
MPII-2.8	Does the device allow the internal media to be removed by a service technician (e.g., for separate destruction or customer retention)?	Yes	__

MPII-2.9	Does the device allow personally identifiable information records be stored in a separate location from the device's operating system (i.e. secondary internal drive, alternate drive partition, or remote storage location)?	No	
MPII-3	Does the device have mechanisms used for the transmitting, importing/exporting of personally identifiable information?	Yes	__
MPII-3.1	Does the device display personally identifiable information (e.g., video display, etc.)?	Yes	__
MPII-3.2	Does the device generate hardcopy reports or images containing personally identifiable information?	No	__
MPII-3.3	Does the device retrieve personally identifiable information from or record personally identifiable information to removable media (e.g., removable-HDD, USB memory, DVD-R/RW,CD-R/RW, tape, CF/SD card, memory stick, etc.)?	Yes	__
MPII-3.4	Does the device transmit/receive or import/export personally identifiable information via dedicated cable connection (e.g., RS-232, RS-423, USB, FireWire, etc.)?	No	__
MPII-3.5	Does the device transmit/receive personally identifiable information via a wired network connection (e.g., RJ45, fiber optic, etc.)?	Yes	__
MPII-3.6	Does the device transmit/receive personally identifiable information via a wireless network connection (e.g., WiFi, Bluetooth, NFC, infrared, cellular, etc.)?	See Notes	1
MPII-3.7	Does the device transmit/receive personally identifiable information over an external network (e.g., Internet)?	No	__
MPII-3.8	Does the device import personally identifiable information via scanning a document?	No	
MPII-3.9	Does the device transmit/receive personally identifiable information via a proprietary protocol?	No	
MPII-3.10	Does the device use any other mechanism to transmit, import or export personally identifiable information?	No	__

Management of Private Data notes:

1) Mobile X-Ray systems may optionally use WiFi to transmit and receive PII.
All X-Ray systems may optionally use a wireless Bluetooth 2D barcode scanner for scanning patient wristbands.

AUTOMATIC LOGOFF (ALOF)

The device's ability to prevent access and misuse by unauthorized users if device is left idle for a period of time.

ALOF-1	Can the device be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)?	Yes	__
ALOF-2	Is the length of inactivity time before auto-logoff/screen lock user or administrator configurable?	Yes	__

AUDIT CONTROLS (AUDT)

The ability to reliably audit activity on the device.

AUDT-1	Can the medical device create additional audit logs or reports beyond standard operating system logs?	Yes	__
AUDT-1.1	Does the audit log record a USER ID?	Yes	__

AUDT-1.2	Does other personally identifiable information exist in the audit trail?	Yes	
AUDT-2	Are events recorded in an audit log? If yes, indicate which of the following events are recorded in the audit log:	Yes	__
AUDT-2.1	Successful login/logout attempts?	Yes	__
AUDT-2.2	Unsuccessful login/logout attempts?	Yes	__
AUDT-2.3	Modification of user privileges?	Yes	__
AUDT-2.4	Creation/modification/deletion of users?	Yes	__
AUDT-2.5	Presentation of clinical or PII data (e.g. display, print)?	Yes	__
AUDT-2.6	Creation/modification/deletion of data?	Yes	__
AUDT-2.7	Import/export of data from removable media (e.g. USB drive, external hard drive, DVD)?	Yes	__
AUDT-2.8	Receipt/transmission of data or commands over a network or point-to-point connection?	Yes	__
AUDT-2.8.1	Remote or on-site support?	Yes	__
AUDT-2.8.2	Application Programming Interface (API) and similar activity?	Yes	__
AUDT-2.9	Emergency access?	Yes	__
AUDT-2.10	Other events (e.g., software updates)?	Yes	__
AUDT-2.11	Is the audit capability documented in more detail?	No	__
AUDT-3	Can the owner/operator define or select which events are recorded in the audit log?	Yes	2
AUDT-4	Is a list of data attributes that are captured in the audit log for an event available?	Yes	__
AUDT-4.1	Does the audit log record date/time?	Yes	__
AUDT-4.1.1	Can date and time be synchronized by Network Time Protocol (NTP) or equivalent time source?	Yes	__
AUDT-5	Can audit log content be exported?	Yes	__
AUDT-5.1	Via physical media?	Yes	__
AUDT-5.2	Via IHE Audit Trail and Node Authentication (ATNA) profile to SIEM?	Yes	3
AUDT-5.3	Via Other communications (e.g., external service device, mobile applications)?	No	__
AUDT-5.4	Are audit logs encrypted in transit or on storage media?	No	4
AUDT-6	Can audit logs be monitored/reviewed by owner/operator?	Yes	__
AUDT-7	Are audit logs protected from modification?	Yes	__
AUDT-7.1	Are audit logs protected from access?	Yes	
AUDT-8	Can audit logs be analyzed by the device?	Yes	__

Audit Controls Notes:

2) All events are stored in the Windows Event Log. Windows provides some controls for defining which events are recorded.
3) Windows Event Forwarding may be used to forwarded events from the Windows Event Log to a SIEM.
4) Only Administrators may view the Windows Event Log. Windows Protected Event Logging (PEL) may be used to encrypt the event log.

AUTHORIZATION (AUTH)

The ability of the device to determine the authorization of users.

AUTH-1	Does the device prevent access to unauthorized users through user login requirements or other mechanism?	Yes	__
AUTH-1.1	Can the device be configured to use federated credentials management of users for authorization (e.g., LDAP, OAuth)?	Yes	__
AUTH-1.2	Can the customer push group policies to the device (e.g., Active Directory)?	Yes	5
AUTH-1.3	Are any special groups, organizational units, or group policies required?	No	6
AUTH-2	Can users be assigned different privilege levels based on 'role' (e.g., user, administrator, and/or service, etc.)?	Yes	__

AUTH-3	Can the device owner/operator grant themselves unrestricted administrative privileges (e.g., access operating system or application via local root or administrator account)?	Yes	__
AUTH-4	Does the device authorize or control all API access requests?	Yes	__
AUTH-5	Does the device run in a restricted access mode, or ‘kiosk mode’, by default?	Yes	7

Authorization Notes:

5) Refer to group policy documentation for a list of permissable group policy changes.

6) Any required group policies are already applied to the medical device. Refer to documentation for the potential impact of changing these group policies. The required local windows user groups are already configured on the medical device. Domain groups must be mapped to local groups to assign user roles.

7) The device starts in a full screen application mode, although non-adminstrator users may exit to a highly controlled desktop.

CYBER SECURITY PRODUCT UPGRADES (CSUP)

The ability of on-site service staff, remote service staff, or authorized customer staff to install/upgrade device's security patches.

CSUP-1	Does the device contain any software or firmware which may require security updates during its operational life, either from the device manufacturer or from a third-party manufacturer of the software/firmware? If no, answer “N/A” to questions in this section.	Yes	__
CSUP-2	Does the device contain an Operating System? If yes, complete 2.1-2.4.	Yes	__
CSUP-2.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	Yes	__
CSUP-2.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	No	__
CSUP-2.3	Does the device have the capability to receive remote installation of patches or software updates?	Yes	__
CSUP-2.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	No	8
CSUP-3	Does the device contain Drivers and Firmware? If yes, complete 3.1-3.4.	Yes	__
CSUP-3.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	No	__
CSUP-3.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	Yes	__
CSUP-3.3	Does the device have the capability to receive remote installation of patches or software updates?	Yes	__
CSUP-3.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	No	8
CSUP-4	Does the device contain Anti-Malware Software? If yes, complete 4.1-4.4.	Yes	9
CSUP-4.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	Yes	__
CSUP-4.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	No	__

CSUP-4.3	Does the device have the capability to receive remote installation of patches or software updates?	Yes	__
CSUP-4.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	Yes	8, 10
CSUP-5	Does the device contain Non-Operating System commercial off-the-shelf components? If yes, complete 5.1-5.4.	Yes	__
CSUP-5.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	Yes	__
CSUP-5.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	No	__
CSUP-5.3	Does the device have the capability to receive remote installation of patches or software updates?	Yes	__
CSUP-5.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	No	8
CSUP-6	Does the device contain other software components (e.g., asset management software, license management)? If yes, please provide details or refernce in notes and complete 6.1-6.4.	No	__
CSUP-6.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	N/A	__
CSUP-6.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	N/A	__
CSUP-6.3	Does the device have the capability to receive remote installation of patches or software updates?	N/A	__
CSUP-6.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	N/A	__
CSUP-7	Does the manufacturer notify the customer when updates are approved for installation?	Yes	11
CSUP-8	Does the device perform automatic installation of software updates?	Yes	__
CSUP-9	Does the manufacturer have an approved list of third-party software that can be installed on the device?	No	12
CSUP-10	Can the owner/operator install manufacturer-approved third-party software on the device themselves?	Yes	12
CSUP-10.1	Does the system have mechanism in place to prevent installation of unapproved software?	Yes	__
CSUP-11	Does the manufacturer have a process in place to assess device vulnerabilities and updates?	Yes	__
CSUP-11.1	Does the manufacturer provide customers with review and approval status of updates?	Yes	11
CSUP-11.2	Is there an update review cycle for the device?	Yes	__

Cybersecurity Product Upgrade Notes:

8) Updates to the Operating System, Drivers / Firmware, Carestream software, integrated 3rd party software, and the host-based IDS/IPS policies are validated by Carestream before being made available for installation. Updates may be installed by Carestream service personnel, by customers using the Security Roll-Up (SRU) tool available for download from Carestream's website, or automatically through the Carestream Product Update Server based on WSUS. Contract carestream Service for additional information.

9) Carestream ImageView medical devices include a host-based Intrusion Detection / Prevention System (IDS/IPS) to whitelist and sandbox executable software and Windows Defender Anti-Virus with cloud based protection. Updates to the IDS/IPS are typically required only when there are changes to the Carestream software that require an updated whitelist.

10) Updates to Windows Defender policies are automatic. Carestream software is whitelisted to prevent accidental identification as malware.

11) Customers may access the Cybersecurity End User section of the Carestream Service Portal. This provides customers with access to additional product security information, the Security Roll-Up (SRU) Tool to install security patches, and Product Security Advisories. Customers may subscribe to receive automatic email notifications whenever there are new SRU updates or advisories. Contract Carestream Service for access to the Cybersecurity End User section of the Carestream Service Portal.

12) The included host-based IPS whitelists common Anti-Virus software, allowing Windows Defender to be replaced with McAfee, Network Associates, Symantec, or TrendMicro solutions. Installation of other 3rd party software may be performed by authorized Carestream Service Personnel or may require the customer to first replace Carestream's host-based IPS with an alternative solution.

HEALTH DATA DE-IDENTIFICATION (DIDT)

The ability of the device to directly remove information that allows identification of a person.

DIDT-1	Does the device provide an integral capability to de-identify personally identifiable information?	Yes	__
DIDT-1.1	Does the device support de-identification profiles that comply with the DICOM standard for de-identification?	Yes	__

DATA BACKUP AND DISASTER RECOVERY (DTBK)

The ability to recover after damage or destruction of device data, hardware, software, or site configuration information.

DTBK-1	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)?	No	__
DTBK-2	Does the device have a “factory reset” function to restore the original device settings as provided by the manufacturer?	Yes	__
DTBK-3	Does the device have an integral data backup capability to removable media?	Yes	__
DTBK-4	Does the device have an integral data backup capability to remote storage?	No	
DTBK-5	Does the device have a backup capability for system configuration information, patch restoration, and software restoration?	Yes	
DTBK-6	Does the device provide the capability to check the integrity and authenticity of a backup?	Yes	__

EMERGENCY ACCESS (EMRG)

The ability of the device user to access personally identifiable information in case of a medical emergency situation that requires immediate access to stored personally identifiable information.

EMRG-1	Does the device incorporate an emergency access (i.e. “break-glass”) feature?	Yes	13

13) See http://www.medicalimaging.org/wp-content/uploads/2011/02/Break-Glass_-_Emergency_Access_to_Healthcare_Systems.pdf

HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU)

How the device ensures that the stored data on the device has not been altered or destroyed in a non-authorized manner and is from the originator.

IGAU-1	Does the device provide data integrity checking mechanisms of stored health data (e.g., hash or digital signature)?	Yes	__

IGAU-2	Does the device provide error/failure protection and recovery mechanisms for stored health data (e.g., RAID-5)?	No	__

MALWARE DETECTION/PROTECTION (MLDP)

The ability of the device to effectively prevent, detect and remove malicious software (malware).

MLDP-1	Is the device capable of hosting executable software?	Yes	__
MLDP-2	Does the device support the use of anti-malware software (or other anti-malware mechanism)? Provide details or reference in notes.	Yes	14
MLDP-2.1	Does the device include anti-malware software by default?	Yes	__
MLDP-2.2	Does the device have anti-malware software available as an option?	No	__
MLDP-2.3	Does the device documentation allow the owner/operator to install or update anti-malware software?	Yes	__
MLDP-2.4	Can the device owner/operator independently (re-)configure anti-malware settings?	No	15
MLDP-2.5	Does notification of malware detection occur in the device user interface?	Yes	
MLDP-2.6	Can only manufacturer-authorized persons repair systems when malware has been detected?	No	15
MLDP-2.7	Are malware notifications written to a log?	Yes	
MLDP-2.8	Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)?	Yes	15
MLDP-3	If the answer to MLDP-2 is NO, and anti-malware cannot be installed on the device, are other compensating controls in place or available?	N/A	__
MLDP-4	Does the device employ application whitelisting that restricts the software and services that are permitted to be run on the device?	Yes	__
MLDP-5	Does the device employ a host-based intrusion detection/prevention system?	Yes	__
MLDP-5.1	Can the host-based intrusion detection/prevention system be configured by the customer?	No	15
MLDP-5.2	Can a host-based intrusion detection/prevention system be installed by the customer?	Yes	15

Malware Detection / Protection Notes:

14) Carestream ImageView medical devices employ a multi-layered security strategy which includes a host-based Intrusion Detection / Prevention System (IDS/IPS) to whitelist and sandbox (limit file and registry access) executable software, Windows Defender Anti-Virus with cloud-based protection, a software firewall configured to block all ports except those required for the function of the device, a whitelist based web proxy server to prevent browsing to potentially malicious websites, and USB device (DLP) protection.

15) The Carestream host-based IDS/IPS may not be configured by customers. Customers seeking more control or additional logging capabilities in their anti-malware software may replace the Carestrem IDS/IPS with an alternative solution using provided configuration guidelines. Contact Carestream service for additional information.

NODE AUTHENTICATION (NAUT)

The ability of the device to authenticate communication partners/nodes.

NAUT-1	Does the device provide/support any means of node authentication that assures both the sender and the recipient of data are known to each other and are authorized to receive transferred information (e.g. Web APIs, SMTP, SNMP)?	Yes	16
NAUT-2	Are network access control mechanisms supported (E.g., does the device have an internal firewall, or use a network connection white list)?	Yes	__
NAUT-2.1	Is the firewall ruleset documented and available for review?	Yes	__
NAUT-3	Does the device use certificate-based network connection authentication?	No	__

Node Authentication Notes:

16) Windows credentials must be provided before accessing the Web APIs via SSO.

CONNECTIVITY CAPABILITIES (CONN)

All network and removable media connections must be considered in determining appropriate security controls. This section lists connectivity capabilities that may be present on the device.

CONN-1	Does the device have hardware connectivity capabilities?	Yes	__
CONN-1.1	Does the device support wireless connections?	Yes	__
CONN-1.1.1	Does the device support Wi-Fi?	See Notes	17
CONN-1.1.2	Does the device support Bluetooth?	See Notes	18
CONN-1.1.3	Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)?	No	__
CONN-1.1.4	Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)?	See Notes	19
CONN-1.2	Does the device support physical connections?	Yes	__
CONN-1.2.1	Does the device have available RJ45 Ethernet ports?	See Notes	20
CONN-1.2.2	Does the device have available USB ports?	See Notes	21
CONN-1.2.3	Does the device require, use, or support removable memory devices?	See Notes	22
CONN-1.2.4	Does the device support other physical connectivity?	See Notes	23
CONN-2	Does the manufacturer provide a list of network ports and protocols that are used or may be used on the device?	Yes	__
CONN-3	Can the device communicate with other systems within the customer environment?	Yes	__
CONN-4	Can the device communicate with other systems external to the customer environment (e.g., a service host)?	See Notes	24
CONN-5	Does the device make or receive API calls?	Yes	__
CONN-6	Does the device require an internet connection for its intended use?	No	__
CONN-7	Does the device support Transport Layer Security (TLS)?	Yes	__
CONN-7.1	Is TLS configurable?	Yes	
CONN-8	Does the device provide operator control functionality from a separate device (e.g., telemedicine)?	No	__

Connectivity Capabilities Notes:

17) WiFi is an available option for Mobile X-Ray systems.

18) Bluetooth is supported only when the optional 2D wireless barcode scanner is in use.

19) X-Ray detectors may be used in wired or wireless mode. Wireless detectors use 802.11g/n.

RF is supported only when the optional wireless exposure switch is in use.

20) Mobile X-Ray systems have an unused RJ45 port when they are not connected to a wired network.

21) Availability of open USB ports is determined by the number of optional features that are enabled on the system.

DLP settings may be enabled to prevent the use of removable storage devices.

22) Patient data may be saved to CD, DVD, or USB media using the optional DICOMDIR (IHE Portable Data for Imaging) feature.
23) Legacy systems upgraded to the ImageView software platform may use a serial connection to the X-Ray generator.
24) The system may optionally communicate with the Remote Management Service (RMS) system, managed by PTC ThingWorx.

PERSON AUTHENTICATION (PAUT)

The ability to configure the device to authenticate users.

PAUT-1	Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)?	Yes	__
PAUT-1.1	Does the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)?	Yes	__
PAUT-2	Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, etc.)?	Yes	__
PAUT-3	Is the device configurable to lock out a user after a certain number of unsuccessful logon attempts?	Yes	__
PAUT-4	Are all default accounts (e.g., technician service accounts, administrator accounts) listed in the documentation?	Yes	__
PAUT-5	Can all passwords be changed?	Yes	__
PAUT-6	Is the device configurable to enforce creation of user account passwords that meet established (organization specific) complexity rules?	Yes	__
PAUT-7	Does the device support account passwords that expire periodically?	Yes	__
PAUT-8	Does the device support multi-factor authentication?	Yes	__
PAUT-9	Does the device support single sign-on (SSO)?	Yes	__
PAUT-10	Can user accounts be disabled/locked on the device?	Yes	__
PAUT-11	Does the device support biometric controls?	Yes	__
PAUT-12	Does the device support physical tokens (e.g. badge access)?	Yes	__
PAUT-13	Does the device support group authentication (e.g. hospital teams)?	Yes	__
PAUT-14	Does the application or device store or manage authentication credentials?	See Notes	25
PAUT-14.1	Are credentials stored using a secure method?	Yes	25

Person Authentication Notes:

25) Credentials are managed by the Windows 10 OS or the Active Directory Domain Service.

PHYSICAL LOCKS (PLOK)

Physical locks can prevent unauthorized users with physical access to the device from compromising the integrity and confidentiality of personally identifiable information stored on the device or on removable media

PLOK-1	Is the device software only? If yes, answer “N/A” to remaining questions in this section.	No	__
PLOK-2	Are all device components maintaining personally identifiable information (other than removable media) physically secure (i.e., cannot remove without tools)?	See Notes	26
PLOK-3	Are all device components maintaining personally identifiable information (other than removable media) physically secured behind an individually keyed locking device?	See Notes	26
PLOK-4	Does the device have an option for the customer to attach a physical lock to restrict access to removable media?	See Notes	26

Physical Locks Notes:

26) The physical locking characteristics will vary with the X-Ray system:
- Mobile Systems: The PC is located behind the covers of the mobile X-Ray system. Tools are required to remove the covers and to remove the co
- Mobile Retrofit Systems: The PC is mounted to an existing mobile X-Ray system. Tools are required to remove the computer. A cable lock may b
- In-Room Systems: The PC is located in the control room for an X-Ray room. A physical lock may be used to prevent opening the computer case. /

ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP)

Manufacturer's plans for security support of third-party components within the device's life cycle.

RDMP-1	Was a secure software development process, such as ISO/IEC 27034 or IEC 62304, followed during product development?	Yes	__
RDMP-2	Does the manufacturer evaluate third-party applications and software components included in the device for secure development practices?	Yes	__
RDMP-3	Does the manufacturer maintain a web page or other source of information on software support dates and updates?	Yes	__
RDMP-4	Does the manufacturer have a plan for managing third-party component end-of-life?	Yes	__

SOFTWARE BILL OF MATERIALS (SBoM)

A Software Bill of Material (SBoM) lists all the software components that are incorporated into the device being described for the purpose of operational security planning by the healthcare delivery organization. This section supports controls in the RDMP section.

SBOM-1	Is the SBoM for this product available?	Yes	__
SBOM-2	Does the SBoM follow a standard or common method in describing software components?	Yes	__
SBOM-2.1	Are the software components identified?	Yes	__
SBOM-2.2	Are the developers/manufacturers of the software components identified?	Yes	__
SBOM-2.3	Are the major version numbers of the software components identified?	Yes	__
SBOM-2.4	Are any additional descriptive elements identified?	Yes	__
SBOM-3	Does the device include a command or process method available to generate a list of software components installed on the device?	No	__
SBOM-4	Is there an update process for the SBoM?	Yes	__

SYSTEM AND APPLICATION HARDENING (SAHD)

The device's inherent resistance to cyber attacks and malware.

SAHD-1	Is the device hardened in accordance with any industry standards?	Yes	__
SAHD-2	Has the device received any cybersecurity certifications?	No	__
SAHD-3	Does the device employ any mechanisms for software integrity checking	Yes	__
SAHD-3.1	Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer-authorized?	Yes	__

SAHD-3.2	Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the software updates are the manufacturer-authorized updates?	Yes	__
SAHD-4	Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)?	Yes	__
SAHD-5	Is the system configurable to allow the implementation of file-level, patient level, or other types of access controls?	No	__
SAHD-5.1	Does the device provide role-based access controls?	Yes	__
SAHD-6	Are any system or user accounts restricted or disabled by the manufacturer at system delivery?	Yes	__
SAHD-6.1	Are any system or user accounts configurable by the end user after initial configuration?	Yes	__
SAHD-6.2	Does this include restricting certain system or user accounts, such as service technicians, to least privileged access?	Yes	__
SAHD-7	Are all shared resources (e.g., file shares) which are not required for the intended use of the device disabled?	Yes	__
SAHD-8	Are all communication ports and protocols that are not required for the intended use of the device disabled?	Yes	__
SAHD-9	Are all services (e.g., telnet, file transfer protocol [FTP], internet information server [IIS], etc.), which are not required for the intended use of the device deleted/disabled?	Yes	__
SAHD-10	Are all applications (COTS applications as well as OS-included applications, e.g., MS Internet Explorer, etc.) which are not required for the intended use of the device deleted/disabled?	Yes	__
SAHD-11	Can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?	Yes	__
SAHD-12	Can unauthorized software or hardware be installed on the device without the use of physical tools?	Yes	27
SAHD-13	Does the product documentation include information on operational network security scanning by users?	Yes	__
SAHD-14	Can the device be hardened beyond the default provided state?	Yes	__
SAHD-14.1	Are instructions available from vendor for increased hardening?	No	__
SHAD-15	Can the system prevent access to BIOS or other bootloaders during boot?	Yes	__
SAHD-16	Have additional hardening methods not included in 2.3.19 been used to harden the device?	Yes	__

System and Application Hardening Notes:

27) The host-based IPS prevents installation of unauthorized software.
DLP controls may prevent installation of software from removable media.

SECURITY GUIDANCE (SGUD)

Availability of security guidance for operator and administrator of the device and manufacturer sales and service.

SGUD-1	Does the device include security documentation for the owner/operator?	Yes	__

Carestream Health, Inc	ImageView V1.7	AJ8791		27-Sep-2020
SGUD-2	Does the device have the capability, and provide instructions, for the permanent deletion of data from the device or media?	No	__	
SGUD-3	Are all access accounts documented?	Yes	__	
SGUD-3.1	Can the owner/operator manage password control for all accounts?	Yes	__	
SGUD-4	Does the product include documentation on recommended compensating controls for the device?	Yes	__	

HEALTH DATA STORAGE CONFIDENTIALITY (STCF)

The ability of the device to ensure unauthorized access does not compromise the integrity and confidentiality of personally identifiable information stored on the device or removable media.

STCF-1	Can the device encrypt data at rest?	See Notes	28
STCF-1.1	Is all data encrypted or otherwise protected?	See Notes	28
STCF-1.2	Is the data encryption capability configured by default?	No	__
STCF-1.3	Are instructions available to the customer to configure encryption?	No	__
STCF-2	Can the encryption keys be changed or configured?	No	__
STCF-3	Is the data stored in a database located on the device?	Yes	__
STCF-4	Is the data stored in a database external to the device?	No	__

Health Data Storage Confidentiality Notes:

28) Data at Rest (DAR) encryption available through optional FIPS 140-2 Level 2 certified self-encrypting hard drives on most systems.

TRANSMISSION CONFIDENTIALITY (TXCF)

The ability of the device to ensure the confidentiality of transmitted personally identifiable information.

TXCF-1	Can personally identifiable information be transmitted only via a point-to-point dedicated cable?	Yes	__
TXCF-2	Is personally identifiable information encrypted prior to transmission via a network or removable media?	No	__
TXCF-2.1	If data is not encrypted by default, can the customer configure encryption options?	No	__
TXCF-3	Is personally identifiable information transmission restricted to a fixed list of network destinations?	Yes	__
TXCF-4	Are connections limited to authenticated systems?	No	__
TXCF-5	Are secure transmission methods supported/implemented (DICOM, HL7, IEEE 11073)?	No	__

TRANSMISSION INTEGRITY (TXIG)

The ability of the device to ensure the integrity of transmitted data.

TXIG-1	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission?	No	__
TXIG-2	Does the device include multiple sub-components connected by external cables?	Yes	__

	REMOTE SERVICE (RMOT)		
	Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.		
RMOT-1	Does the device permit remote service connections for device analysis or repair?	Yes	__
RMOT-1.1	Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair?	Yes	__
RMOT-1.2	Is there an indicator for an enabled and active remote session?	No	__
RMOT-1.3	Can patient data be accessed or viewed from the device during the remote session?	Yes	__
RMOT-2	Does the device permit or use remote service connections for predictive maintenance data?	Yes	__
RMOT-3	Does the device have any other remotely accessible functionality (e.g. software updates, remote training)?	Yes	__

OTHER SECURITY CONSIDERATIONS (OTHR)

NONE

Notes:

Note 1	Example note. Please keep individual notes to one cell. Please use separate notes for separate information