Manufacturer Disclosure Statement for Medical Device Security -- MDS2

Canon Medical Informatics A/S	Vitrea Read 8.4	2022.03.050	10-Mar-2022

Question ID	Question		See note
DOC-1	Manufacturer Name	Canon Medical Informatics A/S	__
DOC-2	Device Description	Software	__
DOC-3	Device Model	Vitrea Read 8.4	__
DOC-4	Document ID	2022.03.050	__
DOC-5	Manufacturer Contact Information	Krumtappen 4, Etage 3, 2500 Valby, Denmark Marcel Lantinga	__
DOC-6	Intended use of device in network-connected environment:	See Notes	Note 22
DOC-7	Document Release Date	2022-03-10	__
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?	No	__
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)?	Yes	__
DOC-11.1	Does the SaMD contain an operating system?	No	__
DOC-11.2	Does the SaMD rely on an owner/operator provided operating system?	Yes	__
DOC-11.3	Is the SaMD hosted by the manufacturer?	No	
DOC-11.4	Is the SaMD hosted by the customer?	Yes	__
		Yes, No, N/A, or See Note	Note #
	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?	No	
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?	No	Note 23
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?	No	__
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)?	Yes	
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?	Yes	—
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.)?	Yes	Inherited from customer network configuration
MPII-3.7	Does the device transmit/receive personally identifiable information over an external network (e.g., Internet)?	Yes	Inherited from customer network configuration
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?	Yes	
MPII-3.10	Does the device use any other mechanism to transmit, import or export personally identifiable information?	Yes	Note 20

Management of Private Data notes:

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?	No	—
AUDT-2.4	Creation/modification/deletion of users?	No	—
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?	No	—
AUDT-2.8.2	Application Programming Interface (API) and similar activity?	No	—
AUDT-2.9	Emergency access?	No	—
AUDT-2.10	Other events (e.g., software updates)?	Yes	—
AUDT-2.11	Is the audit capability documented in more detail?	See Notes	Note 1
AUDT-3	Can the owner/operator define or select which events are recorded in the audit log?	No	
AUDT-4	Is a list of data attributes that are captured in the audit log for an event available?	See Notes	Note 2
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?	See Notes	Note 3
AUDT-5.1	Via physical media?	Yes	—
AUDT-5.2	Via IHE Audit Trail and Node Authentication (ATNA) profile to SIEM?	See Notes	Note 4
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?	Yes	—
AUDT-6	Can audit logs be monitored/reviewed by owner/operator?	See Notes	Note 5
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?	No	

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)?	See Notes	Note 6
AUTH-1.3	Are any special groups, organizational units, or group policies required?	Yes	—
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?	See Notes	Note 7
AUTH-5	Does the device run in a restricted access mode, or 'kiosk mode', by default?	No	—

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?	Yes	—
CSUP-3	Does the device contain Drivers and Firmware? If yes, complete 3.1-3.4.	No	Note 24
CSUP-3.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	N/A	—
CSUP-3.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	N/A	—
CSUP-3.3	Does the device have the capability to receive remote installation of patches or software updates?	N/A	—
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?	N/A	—
CSUP-4	Does the device contain Anti-Malware Software? If yes, complete 4.1-4.4.	No	—
CSUP-4.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	N/A	—
CSUP-4.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	N/A	—
CSUP-4.3	Does the device have the capability to receive remote installation of patches or software updates?	N/A	—
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?	N/A	—
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?	See Notes	Note 8
CSUP-5.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	Yes	—
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?	Yes	—
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?	See Notes	Note 9
CSUP-8	Does the device perform automatic installation of software updates?	See Notes	Note 10
CSUP-9	Does the manufacturer have an approved list of third-party software that can be installed on the device?	No	__
CSUP-10	Can the owner/operator install manufacturer-approved third-party software on the device themselves?	Yes	__
CSUP-10.1	Does the system have mechanism in place to prevent installation of unapproved software?	No	__
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?	No	__
CSUP-11.2	Is there an update review cycle for the device?	No	__

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?	See Notes	Note 11

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?	No	__
DTBK-3	Does the device have an integral data backup capability to removable media?	No	__
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?	No	
DTBK-6	Does the device provide the capability to check the integrity and authenticity of a backup?	No	__

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?	No	__
	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)?	N/A	__
IGAU-2	Does the device provide error/failure protection and recovery mechanisms for stored health data (e.g., RAID-5)?	N/A	__
	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.	See Notes	Note 12
MLDP-2.1	Does the device include anti-malware software by default?	No	__
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?	No	__
MLDP-2.4	Can the device owner/operator independently (re-)configure anti-malware settings?	No	__
MLDP-2.5	Does notification of malware detection occur in the device user interface?	No	
MLDP-2.6	Can only manufacturer-authorized persons repair systems when malware has been detected?	Yes	
MLDP-2.7	Are malware notifications written to a log?	N/A	
MLDP-2.8	Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)?	Yes	
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?	No	__
MLDP-4	Does the device employ application whitelisting that restricts the software and services that are permitted to be run on the device?	No	__
MLDP-5	Does the device employ a host-based intrusion detection/prevention system?	See Notes	Note 13
MLDP-5.1	Can the host-based intrusion detection/prevention system be configured by the customer?	Yes	
MLDP-5.2	Can a host-based intrusion detection/prevention system be installed by the customer?	Yes	__
	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	—
NAUT-2	Are network access control mechanisms supported (E.g., does the device have an internal firewall, or use a network connection white list)?	No	—
NAUT-2.1	Is the firewall ruleset documented and available for review?	N/A	—
NAUT-3	Does the device use certificate-based network connection authentication?	No	—
	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	Note 27
CONN-1.1	Does the device support wireless connections?	Yes	—
CONN-1.1.1	Does the device support Wi-Fi?	Yes	—
CONN-1.1.2	Does the device support Bluetooth?	No	—
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)?	No	—
CONN-1.2	Does the device support physical connections?	Yes	—
CONN-1.2.1	Does the device have available RJ45 Ethernet ports?	Yes	—
CONN-1.2.2	Does the device have available USB ports?	Yes	—
CONN-1.2.3	Does the device require, use, or support removable memory devices?	Yes	—
CONN-1.2.4	Does the device support other physical connectivity?	Yes	—
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)?	Yes	—
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)?	Yes	—
	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?	No	Note 25
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?	See Notes	Note 14
PAUT-7	Does the device support account passwords that expire periodically?	No	Note 14
PAUT-8	Does the device support multi-factor authentication?	No	
PAUT-9	Does the device support single sign-on (SSO)?	Yes	—
PAUT-10	Can user accounts be disabled/locked on the device?	No	Note 25
PAUT-11	Does the device support biometric controls?	No	—
PAUT-12	Does the device support physical tokens (e.g. badge access)?	No	—
PAUT-13	Does the device support group authentication (e.g. hospital teams)?	No	—
PAUT-14	Does the application or device store or manage authentication credentials?	See Notes	Note 15
PAUT-14.1	Are credentials stored using a secure method?	See Notes	Note 15

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.	Yes	—
PLOK-2	Are all device components maintaining personally identifiable information (other than removable media) physically secure (i.e., cannot remove without tools)?	N/A	—
PLOK-3	Are all device components maintaining personally identifiable information (other than removable media) physically secured behind an individually keyed locking device?	N/A	—
PLOK-4	Does the device have an option for the customer to attach a physical lock to restrict access to removable media?	N/A	—

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?	No	—
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?	No	—
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?	No	—
SAHD-4	Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)?	See Notes	Note 16
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?	No	—
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?	See Notes	Note 21
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?	No	—

SAHD-11	Can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?	N/A	—
SAHD-12	Can unauthorized software or hardware be installed on the device without the use of physical tools?	Yes	—
SAHD-13	Does the product documentation include information on operational network security scanning by users?	No	—
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?	N/A	
SAHD-16	Have additional hardening methods not included in 2.3.19 been used to harden the device?	No	—
	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	Note 26
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?	No	—
	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?	No	—
STCF-1.1	Is all data encrypted or otherwise protected?	No	
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?	N/A	—
STCF-3	Is the data stored in a database located on the device?	Yes	Note 17
STCF-4	Is the data stored in a database external to the device?	Yes	Note 17
	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?	No	—
TXCF-2	Is personally identifiable information encrypted prior to transmission via a network or removable media?	Yes	—
TXCF-2.1	If data is not encrypted by default, can the customer configure encryption options?	Yes	—

TXCF-3	Is personally identifiable information transmission restricted to a fixed list of network destinations?	No	—
TXCF-4	Are connections limited to authenticated systems?	See Notes	Note 18
TXCF-5	Are secure transmission methods supported/implemented (DICOM, HL7, IEEE 11073)?	See Notes	Note 19

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?	Yes	Note 19
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?	N/A	—
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)?	No	—

OTHER SECURITY CONSIDERATIONS (OTHR)

NONE

Notes:

Note 1	The audit trail follows the IHE ATNA profile
Note 2	The attributes captured in audit records are documented in DICOM PS 3.15 section A.5.3 "DICOM Specific Audit Messages"
Note 3	Vitrea Read can be configured to use a compliant external Audit Record Repository. This is recommended. The builtin Audit Record Repository stores the original XML audit messages in a DB2 database table and they can be exported using standard DB2 database tools
Note 4	Audit messages can be routed via syslog RFC-3164 or RC-5424 with TLS encryption as per the IHE ATNA profile
Note 5	Audit messages can only be viewed by owner/operator when using the builtin Audit Record Repository. The recommendation is to use an external ARR.
Note 6	User privileges can be controlled via Active Directory groups
Note 7	A few select API end points are deliberately unauthenticated. For instance to allow uploading client logs.

Note 8	The COTS libraries shipped with Vitrea Read are updated with Vitrea Read releases and hotfixes. Updates of the (DB2) database are handled by Canon Medical Informatics CS engineers.
Note 9	OS level updates are generally allowed
Note 10	OS updates are not automatically triggered, but it only requires a single command to install all available updates.
Note 11	Compliance with the DICOM standard for de-identification has not been verified, but said standard has been the guideline for the implementation
Note 12	The customer may on request receive permission to install anti-malware software on the servers that run Vitrea Read
Note 13	The RHEL/CentOS OS provides mechanisms that can be configured. The Vitrea Read clients are installed on the customers PCs as normal unprivileged Windows applications. The security of these PCs is the responsibility of the customer.
Note 14	The system does not enforce any organizationally set password policy for complexity or expiration when configured to use local users. When configured to use Active Directory (the norm) the password policy is managed by Active Directory. Users cannot change their password via Vitrea Read.
Note 15	Vitrea Read stores credentials for locally created users, but not for Active Directory users.
Note 16	The software is installed via MSIs on Windows and via RPMs on Linux. The "rpm -V" can be used to check whether the installation has been tampered with, but there is no protection aganist tampering with the rpm database itself.
Note 17	It is possible to use both a database managed as part of Vitrea Read and an external database.
Note 18	Image retrieval is possible from external unauthenticated sources. The Vitrea Read integration APIs is flexible and could be used to communicate with unauthenticated sources. Vitrea Read itself does not provide unauthenticated access.
Note 19	All external systems accessed using the HTTP protocol can be confgiured to use TLS (HTTPS). DICOM image retrieval over TLS is not supported.
Note 20	Vitrea Read receives and transmits personally identifiable information via the DICOM protocol.
Note 21	Many administrative tasks can be managed via the graphical user interface. Advanced tasks such as software upgrades and daemon configuration requires shell access. Shell access comes in only two levels - miaccess which can only view and root which has full unrestricted access.

Note 22	Vitrea Read PACS system is a Diagnostic Softcopy Reading software package to be used for primary diagnosis and clinical review of digital radiology images (including digital breast tomosynthesis/mammography). Vitrea Read allows diagnostic viewing of fused dual modality studies in a single view. Vitrea Read software is indicated for use by qualified healthcare professionals including, but not restricted to, radiologists, non-radiology specialists, physicians and technologists. The product interfaces to existing imaging equipment using the DICOM standard communication protocol. When viewing mammographic images and other medical images for diagnostic purposes the display monitors used must meet technical specifications and comply with the applicable country specific regulatory approvals and quality requirements. Lossy compressed mammographic images and digitized film screen images must not be reviewed for primary image interpretations. Vitrea Read does not permanently store or produce original medical images or use irreversible compression methods. Vitrea Read is not intended to be used on tablets and smartphones.
Note 23	Vitrea Read does not store patient or image related information in its own database. Only settings and preferences are stored. If Vitrea Read is not configured with Active Directory, Vitrea Read also has information stored about users in its users database. If the deprecated Vitrea Read Audit Record Repository is used the audit database will contain information such as patient IDs and user account names
Note 24	Vitrea Read is installed on servers, physical or virtual, acquired by the customer. The servers run CenOS/RHEL and maintenance is done according to normal best practices. The operating system is not part of the product.
Note 25	The standard enterprise deployment configuration uses Active Directory, which may be configured to lock out users after a number of failed authentication attempts and which also has UI to disable user accounts.
Note 26	The relevant documents are " Vitrea Read Administration Guide" and "Vitrea Read Security Manual"
Note 27	Vitrea Read is software and the server installations typically run on servers with wired ethernet. Client installations run on Windows PCs which can have any kind of network connectivity - wired and wireless