Manufacturer Disclosure Statement for Medical Device Security -- MDS2

Schiller AG Cardiopluse Prime Version 1.2.0 091-0387-00 Rev A 30-Jun-2022

Question ID	Question		See note
DOC-1	Manufacturer Name	Schiller AG	__
DOC-2	Device Description	CardioPluse Prime Version 1.2.0 is a 12-lead electrocardiograph device intended to be used by or under the direct supervision of a licensed healthcare practitioner in healthcare facilities to acquire ECG signals from body surface electrodes, record, analyse, display and print ECGs for diagnosis in adult and paediatric patients.	__
DOC-3	Device Model	98310	__
DOC-4	Document ID	091-0387-00 Rev A	__
DOC-5	Manufacturer Contact Information	SCHILLER AG Altgasse 68 CH-6341 Baar, Switzerland	__
DOC-6	Intended use of device in network-connected environment:	Cardiopulse Prime is intended for indoor use in healthcare facilities.	__
DOC-7	Document Release Date	30-06-2022	__
DOC-8	Coordinated Vulnerability Disclosure: Does the manufacturer have a vulnerability disclosure program for this device?	No	__
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?	No	__
DOC-11.2	Does the SaMD rely on an owner/operator provided operating system?	No	__
DOC-11.3	Is the SaMD hosted by the manufacturer?	No	
DOC-11.4	Is the SaMD hosted by the customer?	No	__

		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	Patient demographic data such as: patient name, birthdate, weight height, ethnicity, gender plus related health information such as ecg waveforms / interpretation statements
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	Stored in local DB

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	Download patient demographic data via PDQ or download worklists which includes patient information and upload of recordings from/to Schiller Server via LAN / WLAN. Import/Export of data in the maintenance workflow.
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	__
MPII-3.7	Does the device transmit/receive personally identifiable information over an external network (e.g., Internet)?	Yes	If the Schiller Server is located outside the hospital infrastructure AND the hospital IT infrastructure does allow this
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:

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	Forced reauthentication is disabled while a recording is taken (e.g. during resting rhythm data acquisition)
ALOF-2	Is the length of inactivity time before auto-logoff/screen lock user or administrator configurable?	Yes	Logoff time is configurable.

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	patient-id and visit-id if audit object is related to a recording
AUDT-2	Are events recorded in an audit log? If yes, indicate which of the following events are recorded in the audit log:	Yes	Start-up of Device, Shutdown of Device, Create Recording, Delete Recording
AUDT-2.1	Successful login/logout attempts?	No	__
AUDT-2.2	Unsuccessful login/logout attempts?	No	__
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)?	No	__
AUDT-2.6	Creation/modification/deletion of data?	Yes	create / delete a patient's recording

AUDT-2.7	Import/export of data from removable media (e.g. USB drive, external hard drive, DVD)?	No	__
AUDT-2.8	Receipt/transmission of data or commands over a network or point-to-point connection?	No	__
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)?	No	__
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?	No	
AUDT-4	Is a list of data attributes that are captured in the audit log for an event available?	No	__
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	Can be synced if Schiller Server or SchillerLink is used as EMR Integration using proprietary API of Schiller Server
AUDT-5	Can audit log content be exported?	Yes	__
AUDT-5.1	Via physical media?	Yes	Can be exported to an attached USB memory stick
AUDT-5.2	Via IHE Audit Trail and Node Authentication (ATNA) profile to SIEM?	No	__
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	__
AUDT-6	Can audit logs be monitored/reviewed by owner/operator?	No	__

AUDT-7	Are audit logs protected from modification?	Yes	The underlying OS cannot be accessed by the user. It is therefore not possible for a user to change the audit log data on the device storage itself. If the device log is exported to a USB memory stick, the
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	Depending on the access configuration, the device uses either a single password, an internal user management with user name and password or the user management provided by the Schiller Server which may be connected to an LDAP system, using user name and password with an associated privilege(s)
AUTH-1.1	Can the device be configured to use federated credentials management of users for authorization (e.g., LDAP, OAuth)?	Yes	Access control can be set to Schiller Server and this server can be configured to use an LDAP / AD system
AUTH-1.2	Can the customer push group policies to the device (e.g., Active Directory)?	Yes	Mapping is done on Schiller Server
AUTH-1.3	Are any special groups, organizational units, or group policies required?	No	Mapping is done on Schiller Server
AUTH-2	Can users be assigned different privilege levels based on 'role' (e.g., user, administrator, and/or service, etc.)?	Yes	Mapping is done on Schiller Server

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)?	No	__
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	The underlying OS of the device is not accessible by the user. The device starts only the ecg recording UI which is the only way to interact with the device.

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?	No	Software updates can be stored on a server (Schiller Update Server) but the update has to be started manually on the device. It is not possible to start an update from a remote system.
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	__
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?	Yes	__
CSUP-3.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	No	__
CSUP-3.3	Does the device have the capability to receive remote installation of patches or software updates?	No	__
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	__
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.	No	__
CSUP-5.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	N/A	__
CSUP-5.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	N/A	__
CSUP-5.3	Does the device have the capability to receive remote installation of patches or software updates?	N/A	__
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?	N/A	__
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	__
CSUP-8	Does the device perform automatic installation of software updates?	No	__
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?	No	__
CSUP-10.1	Does the system have mechanism in place to prevent installation of unapproved software?	Yes	The underlying OS of the device is not accessible by the user. The device starts only the ecg recording UI which is the only way to interact with the device.
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?	No	__
DIDT-1.1	Does the device support de-identification profiles that comply with the DICOM standard for de-identification?	No	__

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	Data can be stored on the device. But for long time storage, integration to a Schiller Server or SchillerLink is needed.
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?	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?	Yes	Possibility to acquire a resting ecg without providing authentication, but patient data cannot be retrieved

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)?	No	Integrity of recording files (ecg data) is checked with an MD5 hash. Integrity of patient recordings (stored in internal database) is not checked.
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?	No	__
MLDP-2	Does the device support the use of anti-malware software (or other anti-malware mechanism)? Provide details or reference in notes.	No	__
MLDP-2.1	Does the device include anti-malware software by default?	N/A	__
MLDP-2.2	Does the device have anti-malware software available as an option?	N/A	__
MLDP-2.3	Does the device documentation allow the owner/operator to install or update anti-malware software?	N/A	__
MLDP-2.4	Can the device owner/operator independently (re-)configure anti-malware settings?	N/A	__
MLDP-2.5	Does notification of malware detection occur in the device user interface?	N/A	
MLDP-2.6	Can only manufacturer-authorized persons repair systems when malware has been detected?	N/A	
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)?	N/A	
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?	Yes	The OS is locked down (kiosk mode) so that users cannot install new software.
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?	No	__
MLDP-5.1	Can the host-based intrusion detection/prevention system be configured by the customer?	N/A	__

MLDP-5.2	Can a host-based intrusion detection/prevention system be installed by the customer?	N/A	__

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	SSL Certificate validation is optional, client authenticates with user name and password
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	Device does not offer any network services, all sockets are closed. Exception: If SchillerLink integration is configured, a RESTful endpoint is run on the device.
NAUT-2.1	Is the firewall ruleset documented and available for review?	No	__
NAUT-3	Does the device use certificate-based network connection authentication?	Yes	Supported through WPA2 Enterprise

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?	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	Export PDF Reports, Import & Export Settings, Update Firmware, Export Recordings, Export Audit Trail and Log files. Connect Bar Code scanner via USB for patient data entry.
CONN-1.2.3	Does the device require, use, or support removable memory devices?	Yes	Export PDF Reports, Import Settings, Update Firmware, Export Recordings via a removable USB memory stick
CONN-1.2.4	Does the device support other physical connectivity?	No	__
CONN-2	Does the manufacturer provide a list of network ports and protocols that are used or may be used on the device?	No	__
CONN-3	Can the device communicate with other systems within the customer environment?	Yes	Via SchillerServer or SchillerLink through LAN or WiFi
CONN-4	Can the device communicate with other systems external to the customer environment (e.g., a service host)?	No	__
CONN-5	Does the device make or receive API calls?	Yes	If EMR integration is active: Schiller Server: Calls RESTful interface on Schiller Server SchillerLInk: Calls RESTful interface on Schiller Link server and allows to receive API calls on internal RESTful service.

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?	No	
CONN-8	Does the device provide operator control functionality from a separate device (e.g., telemedicine)?	No	__

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)?	See Notes	The device can be configured to use either a local user database or the ldap. Service account is not unique
PAUT-1.1	Does the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)?	No	The device can be configured such that no access control is active!
PAUT-2	Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, etc.)?	Yes	Using AccessControl set to SchillerServer it is possible to authenticate through LDAP / Active Directory
PAUT-3	Is the device configurable to lock out a user after a certain number of unsuccessful logon attempts?	See Notes	If AccessControl is set to SchillerServer and LDAP /Active Directory is configured such to block the user account it is possible to lock out a user (in the system)
PAUT-4	Are all default accounts (e.g., technician service accounts, administrator accounts) listed in the documentation?	See Notes	

PAUT-5	Can all passwords be changed?	See Notes	All passwords (for local or basic accesscontrol) an be changed (except the password for service account)
PAUT-6	Is the device configurable to enforce creation of user account passwords that meet established (organization specific) complexity rules?	No	__
PAUT-7	Does the device support account passwords that expire periodically?	No	If LDAP via SchillerServer is used, account password expiration can be configured via the LDAP server.
PAUT-8	Does the device support multi-factor authentication?	No	__
PAUT-9	Does the device support single sign-on (SSO)?	No	__
PAUT-10	Can user accounts be disabled/locked on the device?	No	__
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)?	See Notes	If LDAP via SchillerServer is used,group to role maapings are possible
PAUT-14	Does the application or device store or manage authentication credentials?	Yes	If access control mode “local” is configured, the user accounts are configured and stored on the device.
PAUT-14.1	Are credentials stored using a secure method?	Yes	Passwords are stored as hash with a salt

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)?	Yes	__
PLOK-3	Are all device components maintaining personally identifiable information (other than removable media) physically secured behind an individually keyed locking device?	No	__
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	Schiller SW development process according IEC 62304 and applied Cybersecurity Process
RDMP-2	Does the manufacturer evaluate third-party applications and software components included in the device for secure development practices?	No	__
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	Postmarket Surveillance covers the monitoring and management of third party components

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	See Work-sheet SBOM List
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?	Yes	Within the Info section of the device menu, the Schiller components are listed but not the SOUPs
SBOM-4	Is there an update process for the SBoM?	Yes	Within the Info section of the device menu, the Schiller components are listed but not the SOUPs

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	During software update process the software update package is checked
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?	Yes	__
SAHD-4	Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)?	No	__
SAHD-5	Is the system configurable to allow the implementation of file-level, patient level, or other types of access controls?	Yes	__
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	If the access control mode “local” is active multiple users with different access levels are predefined.
SAHD-6.1	Are any system or user accounts configurable by the end user after initial configuration?	Yes	If access control mode “local” is configured, the administrator can add, remove or modify user accounts on the device.
SAHD-6.2	Does this include restricting certain system or user accounts, such as service technicians, to least privileged access?	Yes	Exception: Maintenance mode can always be accessed using a non-changeable password.
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)?	See Notes	The device allows to boot a recovery image from USB memory stick. This functionality cannot be disabled.
SAHD-12	Can unauthorized software or hardware be installed on the device without the use of physical tools?	No	__
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?	No	__
SAHD-14.1	Are instructions available from vendor for increased hardening?	N/A	
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?	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	IFU contains such information
SGUD-2	Does the device have the capability, and provide instructions, for the permanent deletion of data from the device or media?	Yes	IFU contains informtion how - local users can be deleted - local recordings can be deleted
SGUD-3	Are all access accounts documented?	N/A	
SGUD-3.1	Can the owner/operator manage password control for all accounts?	N/A	__
SGUD-4	Does the product include documentation on recommended compensating controls for the device?	See Notes	The IFU contains information regarding network safety in chapter 1.12 of the IFU

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?	_______	__
STCF-1.1	Is all data encrypted or otherwise protected?		
STCF-1.2	Is the data encryption capability configured by default?		
STCF-1.3	Are instructions available to the customer to configure encryption?		

STCF-2	Can the encryption keys be changed or configured?	_______	__
STCF-3	Is the data stored in a database located on the device?	_______	Device is using embedded DB Sqlite
STCF-4	Is the data stored in a database external to the device?	_______	__

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?	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	Communication only possible with SchillerServer and SchillerLink
TXCF-4	Are connections limited to authenticated systems?	Yes	Remote system SSL certificate is validated.
TXCF-5	Are secure transmission methods supported/implemented (DICOM, HL7, IEEE 11073)?	Yes	Restful over TLS

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	No special mechanism aside of the integrity ensured by the TLS protocol.
TXIG-2	Does the device include multiple sub-components connected by external cables?	No	__

	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?	No	__
RMOT-1.1	Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair?	N/A	__
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?	N/A	__
RMOT-2	Does the device permit or use remote service connections for predictive maintenance data?	No	__
RMOT-3	Does the device have any other remotely accessible functionality (e.g. software updates, remote training)?	No	__