White Paper

RAPIDPoint 500e Blood Gas System V5.1 and above Security White Paper and MDS²

The facts about the security of our products and solutions

siemens-healthineers.com/rapidpoint500e

SIEMENS Healthineers

Foreword

The Siemens Healthineers Product and Solution Security (PSS) program

At Siemens Healthineers, we are committed to working with you to address cybersecurity and privacy requirements. Our Product and Solution Security Office is responsible for our global program that focuses on addressing cybersecurity throughout the product lifecycle.

Our program targets incorporating state-of-the-art cybersecurity into our current and future products. We seek to protect the security of your data while providing measures to strengthen the resiliency of our products from cyber threats.

We comply with applicable security and privacy regulations from the U.S. Department of Health and Human Services (HHS), including the Food and Drug Administration (FDA) and Office for Civil Rights (OCR), to help you meet your IT security and privacy obligations.

Vulnerability and incident management

Siemens Healthineers cooperates with government agencies and cybersecurity researchers concerning reported potential vulnerabilities. Our communications policy strives for coordinated disclosure. We work in this way with our customers and other parties, when appropriate, in response to potential vulnerabilities and incidents in our products, no matter the source.

Elements of our product and solution security program

- Providing information to facilitate secure configuration and use of our medical devices in your IT environment
- Conducting formal threat and risk analysis for our products
- Incorporating secure architecture, design, and coding methodologies in our software development process
- Performing static code analysis of our products
- Conducting security testing of products under development as well as products already in the field
- Tailoring patch management to the medical device and depth of coverage chosen by you
- Monitoring security vulnerability to track reported third-party component issues in our products
- Working with suppliers to address security throughout the supply chain
- Training of employees to provide knowledge consistent with their level of responsibilities regarding your data and device integrity

Contacting Siemens Healthineers about product and solution security

Siemens Healthineers requests that you report any cybersecurity or privacy incidents by email to: productsecurity@siemens-healthineers.com

Contents

Basic Information

Depend on the RAPIDPoint® 500e Blood Gas System to raise the bar in blood gas IT security at your facility by providing the latest defenses to guard confidential patient data coupled with the leading built-in technology to protect your institution from external cybersecurity threats.

Operating systems

- WINDOWS 10 IoT Enterprise (1809) (user interface processor)
- pSOS+ Version 2.3 (real-time processor)

Hardware specifications

- BlueChip Technology AMD GLX ETX module with 1 GB RAM (user interface processor)
- Motorola 68332 (real-time processor)

User account information

- Single operating system local administrator-level account (auto-login) for running instrument application. Note: Account has no privileges beyond the boundaries of the instrument.
- Operators of the system can be created (up to 5000 unique operators) and granted one of four levels of access privileges.

Patching strategy

Operating system updates are evaluated and included as part of application software updates. Registered customers have access to the fleet template at https://fleet.siemens-healthineers.com/welcome

Cryptography usage

- Patient data export files can (optionally) be encrypted using AES-256 encryption provided by 7-Zip.
- Data on the hard drive is encrypted via BitLocker using the Trusted Platform Module (TPM).
- Communication with the POCcelerator™ Data Management System can be configured to encrypt LIS communication.

Handling of sensitive data

Patient and sample demographic data can be entered via the on-screen data entry forms. Additionally, some patient demographic data can be retrieved from data management systems based on matching patient ID.

Patient demographic data consists of the following entries: Patient ID (used as a key that links to all other patient demographic fields), Last Name, First Name, Gender, and Date of Birth.

Sample demographic data consists of the following entries: Location, Physician ID, Sample Draw Date, Sample Draw Time, Accession Number, Operator ID, Temperature, entered tHb (available only when measured tHb is turned off), FIO2, Flow, Respiratory Rate, Barometric Pressure, CPAP, PEEP, PIP, Tidal Volume, and Allen Test result. In addition, the system can be configured to support up to 10 user-defined demographic entry fields, limited to 15 characters per label and 15 characters per value.

Demographic data associated with samples can be configured in Setup to deselect fields (so data is not collected), select fields (so data can be collected), or be indicated as required fields (so data must be collected prior to releasing sample results).

Raw (second-by-second) and reportable result data is stored in a combination of database entries augmented with binary "sideband" files. No sensitive information is included in diagnostic logs.

When data is exported for reliability analysis by Siemens Healthineers, the patient and sample demographic database tables are omitted from the export files. However, traceability of data to patient ID or accession number is included in case it is needed for field issue investigations.

Data is purged in first-in, first-out (FIFO) order. For patient samples, the instrument maintains the last 1250 samples (allowing up to 100 additional records prior to triggering the purge operation). However, only the most recent 250 patient samples are viewable on the instrument by the operator.

Data recovery

The RAPIDPoint 500e system is a data producer and is not intended for long-term storage of data. As such, it provides limited data backup options and no data restore capability.

Long-term data storage is provided by external data management systems, such as the POCcelerator Data Management System.

Device configuration (setup) data can be saved to and restored from removable USB media by level 1 (administrator-level) operators.

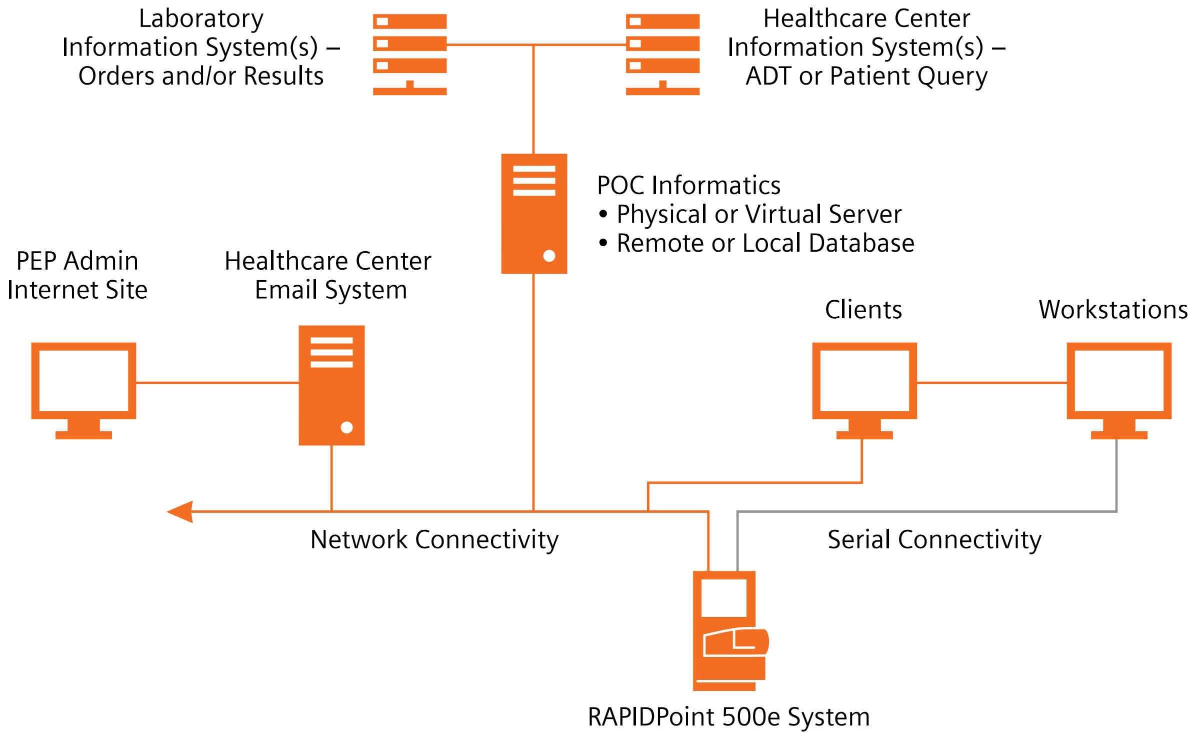
Boundary defense

The WINDOWS Firewall, enabled by default, is used to limit network traffic to the device. Additionally, endpoint identification can be used to further restrict laboratory information system (LIS) and Remote Viewer (VNC) communication to a user-defined list of IP addresses or subnets. It is anticipated that the device will be operated on an internal, non-public-facing network to further reduce the risk of network intrusion.

Terms and conditions

See local terms and conditions for purchasing and operating this device within your area.

Network Information


Laboratory Information System(s) – Orders and/or Results
Healthcare Center Information System(s) – ADT or Patient Query
POC Informatics
• Physical or Virtual Server
• Remote or Local Database
PEP Admin Internet Site
Healthcare Center Email System
Clients
Workstations
Network Connectivity
Serial Connectivity
RAPIDPoint 500e System

The server requires no static IP addresses but may be configured in static IP address mode if desired by the facility. The following ports are used by the system:

Port Number	Service/function	Direction (in/out)	Protocol
25	SMTP email (optional)	Out	SMTP
3001*	Unencrypted LIS communication with data manager (*Port number is user-configurable)	In	LIS3/LIS4
3001*	Encrypted LIS communication with Siemens Healthineers data manager (*Port number is user-configurable)	Out	LIS3/LIS4
5355	Link-Local Multicast Name Resolution (used by some SMTP servers for email negotiation)	Out	LLMNR
5900	Remote Viewer	In	VNC

Allowed services accessible through network:

Service	Description	Startup Type	Log on as:
VNC	Virtual Network Computing used for Remote View (available only on Siemens Healthineers data managers)	User-configurable. Startup is deferred until connection to Siemens Healthineers data manager has been established.	User-configurable

Security Controls

Malware protection

McAfee Embedded Control (whitelisting solution) creates a list of trusted programs necessary for day-to-day operations and ensures that only those specific applications are allowed to run.

Controlled use of administrative privileges

- System runs in kiosk mode, preventing user access to the underlying operating system.
- System automatically logs in using administrative account, but account has privileges only on the local machine.

Authentication

- Supports password only or operator ID and password user authentication.
- Allows up to 5000 unique operator IDs for nonambiguous identification of personnel.
- Includes four role-based permission levels: System Supervisor, Key Operator, Routine Operator, Occasional Operator.
- Provides three modes of system access: Restricted, Limited, Unrestricted.

Security scanning

Prior to release, all media is scanned to confirm the absence of malware using Trend Micro OfficeScan. In addition, the system was scanned by Siemens Extensible Security Testing Appliance (SiESTA), which includes Nessus 8.8.0.

Continuous vulnerability monitoring

- Components of the system are registered with the Siemens Healthineers CERT Software Vulnerability Monitoring system, which notifies product engineering when vulnerabilities are reported by component vendors.
- Vulnerabilities are tracked via the defect tracking process for the product, assessed for relevance and applicability, and then enter the Complaint Escalation Review process to determine next steps.

Hardening

The instrument uses an embedded operating system that allows control of which components are included and excluded in the OS image, minimizing the attack surface.

- Unnecessary ports and services have been disabled.
- System is configured in kiosk mode to prevent access to the underlying operating system.
- Access to the internet via the instrument is prevented, limiting exposure to common attacks.
- Auto-launch of executables when removable media is inserted has been disabled.

Network controls

- WINDOWS Firewall is enabled by default.
- Endpoint identification can be applied to limit addresses allowed to connect for LIS and Remote Viewer traffic.
- ICMP protocol is limited to a subset of supported messages (ping request/reply only).

Physical safeguards

- The RAPIDPoint 500e instrument should reside and be operated in a physically controlled environment.
- The PS/2 keyboard port is not exposed.
- The USB hub is not powered until the instrument application is running.
- USB hub power can be configured as off by the System Supervisor except for Level 1 operations such as Save/Restore Setup and Software Installation.

Data protection controls

- Data on the hard drive is encrypted via BitLocker using the Trusted Platform Module (TPM).
- The ability to edit patient and sample demographics in Data Recall is disabled by default.
- Patient sample data exported to comma-separated value (CSV) files is, by default, encrypted with a user-provided encryption password. When encryption is disabled, a warning is displayed on the export screen.
- Communication with the POCcelerator Data Management System can be configured to encrypt LIS communication. If unencrypted LIS communication is in use, a warning icon is displayed in the screen header.
- When data is exported for reliability analysis by Siemens Healthineers, the patient and sample demographic database tables are omitted from the export files. However, traceability of data to patient ID or accession number is included in case it is needed for field issue investigations.

Auditing/logging

Event logging tracks some key user activities. Event information can only be viewed after post-processing by Field Service.

Remote connectivity

- Connection to an external data manager is available via TCP connection (on port 3001 by default, configurable by the facility). Connection to the POCcelerator Data Management System can be encrypted using a certificate managed by the POCcelerator system.
- VNC (Remote Viewer) connection is available (exclusive to Siemens Healthineers data managers).
- Outbound-only email is available to facilitate transmission of data to Siemens Healthineers for reliability analysis (patient demographic data is omitted from transmitted data).

Shared Responsibilities

Administrative controls
Certain features are accessible only to System Supervisor-level operators, including the following:

- System access mode
- Operator management
- Editing of correlation coefficients
- Software installation
- Saving/restoring of setup data

Incident response and management

- Incidents are managed through the Complaint Escalation Review process.
- When appropriate, the local Product Solutions and Security Officer will initiate a task force to determine response actions and coordinate their execution.

The following are steps that the facility can take to enhance the security of the system:

- Maintain the system in a physically restricted environment to limit access. Only appropriately trained and authorized operators should interact with the system.
- When the system is connected to a network, the network should be an internal, non-public-facing network to further reduce the risk of network intrusion. Access to the internet is not required (or desired).
- If communicating with a Siemens Healthineers data manager, change the Remote Viewer password on both the instrument and the data manager.
- Remove the default System Supervisor account and create unique accounts for all operators. Siemens Healthineers data managers allow operators to be configured and managed centrally (including recertification/password expiration dates) and downloaded to all instruments in the institution. NOTE: When creating passwords, the facility is responsible for defining and enforcing password complexity recommendations.
- Change the System Access control to Restricted to require all operators to sign in prior to use of the system for any purpose.
- Update the software when new versions are provided by Siemens Healthineers.
- Though the WINDOWS login and password are valid only on the local instrument, changing the OS credentials on the system can further inhibit network intrusion.

Software Bill of Materials

The following table lists all third-party technologies used:

Vendor	Component	Component Version	Description/Use
Microsoft	WINDOWS 10 IoT Enterprise 2019 LTSC	1809 (x86)	Operating system
Raima	Raima Data Manager	12.0	Database
McAfee	Embedded Control	8.2.1-114	Anti-malware monitor
7-Zip	7-zip Extra	18.05	File compression with encryption
TightVNC	VNC Server	2.8.23	Remote Viewer screen share
TouchBase	Universal Pointing Device Driver	3.05.18	Touchscreen utilities
Motorola/Zebra	SNAPI.dll	3.0.0.5	USB bar-code reader interface library
OpenSSL.org	OpenSSL	1.1.0l	TLS 1.2 encryption of network LIS traffic
NXP Semiconductors	Background Debug Mode driver	V090	Utility used for programming Motorola 68332 Real-Time Processor
Altera/Intel	Jam STAPL Player	2.2	Utility used for programming FPGA
SourceForge	jwSMTP	1.32	Email utility
Microsoft	Visual C++ 2008 Redistributable Package	x86	Redistributable compiler library binaries
	Visual C++ 2010 Redistributable Package	x86	
	Visual C++ 2013 Redistributable Package	x86	
Raffael Hermann	QR Coder	1.3.6	QR Code generator
Rene’ Nyffenegger	Base64_Encoder	2.rc.04	Base64 encoder

Manufacturer Disclosure Statement (MDS2)

Question ID	Question		See note
DOC-1	Manufacturer Name	Siemens Healthineers	
DOC-2	Device Description	The RAPIDPoint 500e Blood Gas System is intended for in vitro diagnostic use and is designed to provide the determination in whole blood for the following parameters: pH, $p\text{CO}_2$, $p\text{O}_2$, Na^+, K^+, Ca^{++}, Cl^-, Glu, Lac, tHb, FO_2Hb, FCOHb, FMetHb, FHHb, and neonatal bilirubin. The RAPIDPoint 500e Blood Gas System is also intended for in vitro testing of pleural fluid samples for the pH parameter. The Dialysate† option also reports pH, $p\text{CO}_2$, and HCO_3 (calculated) and is for reference information only. *†The dialysate option is not available in the U.S.* This test system is intended for use in point-of-care or laboratory settings.	
DOC-3	Device Model	RAPIDPoint 500e Blood Gas System	
DOC-4	Document ID	DX030640	
DOC-5	Manufacturer Contact Information	https://www.siemenshealthineers.com/how-can-we-help-you	
DOC-6	Intended use of device in network-connected environment	Transmission of results/status with laboratory information system (LIS) or other data management system. Also supports Remote Viewer for Siemens Healthineers data managers via VNC protocol. Optional: Email used for cartridge reliability investigations.	

Question ID	Question		See note
DOC-7	Document Release Date	January 2021	
DOC-8	Coordinated Vulnerability Disclosure: Does the manufacturer have a vulnerability disclosure program for this device?	Yes, see https://new.siemens.com/global/en/products/services/cert/vulnerability-process.html	
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, see Network Information section.	
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	
MPII-1	Can this device display, transmit, store, or modify personally identifiable information (e.g. electronic Protected Health Information (ePHI))?	Yes	See note 1
MPII-2	Does the device maintain personally identifiable information?	Yes	

Question ID	Question		See note
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	See note 2
MPII-2.4	Does the device store personally identifiable information in a database?	Yes	See note 3
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	See note 4
MPII-2.7	Does the device maintain personally identifiable information when powered off, or during power service interruptions?	Yes	

Question ID	Question		See note
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	See note 5
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.)?	Yes	
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.)?	No	
MPII-3.7	Does the device transmit/receive personally identifiable information over an external network (e.g., Internet)?	Yes	See note 6
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	See note 7

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.

Question ID	Question		See note
ALOF-1	Can the device be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., autologoff, session lock, password protected screen saver)?	No	
ALOF-2	Is the length of inactivity time before autologoff/ screen lock user or administrator configurable?	N/A	

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	See note 8
AUDT-1.2	Does other personally identifiable information exist in the audit trail?	No	
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	See note 9
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?	No	
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?	Yes	See note 10
AUDT-2.10	Other events (e.g., software updates)?	Yes	See note 11
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	See note 12
AUDT-5	Can audit log content be exported?	Yes	
AUDT-5.1	Via physical media?	Yes	

Question ID	Question		See note
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)?	Yes	See note 13
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?	No	
AUDT-7.1	Are audit logs protected from access?	No	
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	See note 14
AUTH-1.1	Can the device be configured to use federated credentials management of users for authorization (e.g., LDAP, OAuth)?	No	
AUTH-1.2	Can the customer push group policies to the device (e.g., Active Directory)?	No	
AUTH-1.3	Are any special groups, organizational units, or group policies required?	N/A	
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)?	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	See note 15

Cybersecurity 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	

Question ID	Question		See note
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 vendorauthorized 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	
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 vendorauthorized 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.	Yes	
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 vendorauthorized 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?	No	
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?	No	
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	

Question ID	Question		See note
CSUP-5.2	Does the device require vendor or vendorauthorized 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?	No	
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	
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 vendorauthorized 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	See note 16
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?	N/A	
CSUP-10	Can the owner/operator install manufacturerapproved 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	
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	See note 17
CSUP-11.2	Is there an update review cycle for the device?	Yes	See note 18

Health Data De-Identification (DIDT)

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

Question ID	Question		See note
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?	N/A	

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)?	Yes	
DTBK-2	Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer?	No	See note 19
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?	Yes	See note 20
DTBK-6	Does the device provide the capability to check the integrity and authenticity of a backup?	Yes	See note 21

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	See note 22

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	
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 antimalware software (or other anti-malware mechanism)? Provide details or reference in notes.	Yes	See note 23

Question ID	Question		See note
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?	N/A	
MLDP-2.3	Does the device documentation allow the owner/operator to install or update antimalware software?	No	
MLDP-2.4	Can the device owner/operator independently (re-) configure anti-malware settings?	Yes	See note 24
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	See note 25
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	See note 26
MLDP-3	If the answer to MLDP-2 is NO, and antimalware 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	See note 27
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?	No	

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)?	No	
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	See note 28
NAUT-2.1	Is the firewall ruleset documented and available for review?	Yes	See note 29
NAUT-3	Does the device use certificate-based network connection authentication?	No	

Question ID	Question		See note
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?	No	
CONN-1.1.1	Does the device support Wi-Fi?	No	
CONN-1.1.2	Does the device support Bluetooth?	No	
CONN-1.1.3	Does the device support other wireless network No 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	See note 30
CONN-1.2.3	Does the device require, use, or support removable memory devices?	Yes	See note 31
CONN-1.2.4	Does the device support other physical connectivity?	Yes	See note 32
CONN-2	Does the manufacturer provide a list of network ports and protocols that are used or may be used on the device?	Yes	See note 33
CONN-3	Can the device communicate with other systems within the customer environment?	Yes	See note 34
CONN-4	Can the device communicate with other systems external to the customer environment (e.g., a service host)?	Yes	See note 35
CONN-5	Does the device make or receive API calls?	No	
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	See note 36
CONN-7.1	Is TLS configurable?	No	
CONN-8	Does the device provide operator control functionality from a separate device (e.g., telemedicine)?	Yes	See note 37

Question ID	Question		See note
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	See note 38
PAUT-1.1	Does the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)?	Yes	See note 38
PAUT-2	Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, etc.)?	No	
PAUT-3	Is the device configurable to lock out a user after a certain number of unsuccessful logon attempts?	No	
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?	No	
PAUT-7	Does the device support account passwords that expire periodically?	Yes	See note 39
PAUT-8	Does the device support multi-factor authentication?	No	See note 40
PAUT-9	Does the device support single sign-on (SSO)?	No	
PAUT-10	Can user accounts be disabled/locked on the device?	Yes	See note 41
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?	Yes	See note 42
PAUT-14.1	Are credentials stored using a secure method?	No	
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	

Question ID	Question		See note
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?	No	

Roadmap for Third Party Applications and Software 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	See note 43
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	See note 44
RDMP-4	Does the manufacturer have a plan for managing third-party component end-of-life?	Yes	See note 45

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 note 46
SBOM-2	Does the SBoM follow a standard or common method in describing software components?	Yes	See note 47
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	See note 48

Question ID	Question		See note
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?	No	
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	See note 49
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?	No	
SAHD-5.1	Does the device provide role-based access controls?	Yes	
SAHD-6	Are any system or user accounts Unrestricted 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	See note 50
SAHD-6.2	Does this include restricting certain system or user accounts, such as service technicians, to least privileged access?	No	
SAHD-7	Are all shared resources (e.g., file shares) which are not required for the intended use of the device disabled?	Yes	See note 51
SAHD-8	Are all communication ports and protocols that are not required for the intended use of the device disabled?	Yes	See note 52
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	See note 52
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	

Question ID	Question		See note
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	See note 53
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?	Yes	
SAHD-14.1	Are instructions available from vendor for increased hardening?	Yes	See note 54
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	See note 55

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	See note 56
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?	Yes	See note 57
STCF-1.1	Is all data encrypted or otherwise protected?	Yes	See note 57
STCF-1.2	Is the data encryption capability configured by default?	Yes	
STCF-1.3	Are instructions available to the customer to configure encryption?	N/A	
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	See note 58
STCF-4	Is the data stored in a database external to the device?	No	

Question ID	Question		See note

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	See note 59
TXCF-2.1	If data is not encrypted by default, can the customer configure encryption options?	Yes	
TXCF-3	Is personally identifiable information transmission Unrestricted 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)?	Yes	See note 60

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	See note 60
TXIG-2	Does the device include multiple subcomponents 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?	Yes	See note 61
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?	No	
RMOT-3	Does the device have any other remotely accessible functionality (e.g. software updates, remote training)?	No	

	Other Security Considerations (OTHR)
	NONE

Note	Note
Note 1 MPII-1	List of PII
	The RAPIDPoint 500e system allows for the configuration and optional collection of the following PII data: • Patient ID • Last Name • First Name • Gender • Date of Birth • Location • Physician ID • Draw Date/Time • Accession Number • Operator ID • Temperature • Entered tHb • FIO2 • Flow • Respiration Rate • CPAP • PEEP • PIP • Tidal Volume • Allen Test result • Qt • Up to 10 user-defined demographic entries
Note 2 MPII-2.3	PII preserved until erased.
	The RAPIDPoint 500e system maintains up to 1350 patient sample records, with purging rules that automatically delete records down to 1250 samples.
Note 3 MPII-2.4	PII in database
	The RAPIDPoint 500e system stores patient sample data in a Raima 12.0 database (accessible only on instrument).
Note 4 MPII-2.6	PII import/export with other systems
	The RAPIDPoint 500e system has the option to communicate with a laboratory information system (LIS) or other data management server to transmit patient samples and (optionally) to obtain patient demographics from the remote system based on patient ID. The RAPIDPoint 500e system also allows export of patient sample data to CSV files (which can be optionally encrypted) on removable USB media.
Note 5 MPII-3	Transmitting, importing/exporting PII
	The RAPIDPoint 500e system allows optional communication with a LIS or data export via CSV to USB media.
Note 6 MPII-3.7	Data files sent via email for cartridge reliability investigations include a copy of the Patient ID and Accession Number for the sample.

Note	Note
Note 7 MPII-3.10	Import personally identifiable information
	The RAPIDPoint 500e system allows entry of information using either an integrated or external bar-code scanner.
Note 8 AUDT-1.1	User ID in audit logs
	The RAPIDPoint 500e system audit logs can identify most the recent user sign-in, but not all activities performed by the user nor the date/time of sign-off.
Note 9 AUDT-2.1	Successful login/logout attempts audit
	Only successful logins are audited, not logouts.
Note 10 AUDT-2.9	Emergency access audit
	Login audit only tracks successful logins, but does not track activities performed while logged in.
Note 11 AUDT-2.10	Software update audits
	A text file maintains the update history of the device, including date/time of upgrade and versions before and after.
Note 12 AUDT-4.1.1	Date/Time synchronization
	Communication with laboratory information system (LIS) or data management system allows remote system to query and set date/time on the RAPIDPoint 500e system.
Note 13 AUDT-5.3	Audit log via other communication
	Audit information is part of data transmitted via email for cartridge reliability investigations.
Note 14 AUTH-1	Prevent access to unauthorized users
	The RAPIDPoint 500e system prompts for password (entry via on-screen keyboard or bar code).
Note 15 AUTH-5	Device in kiosk mode
	The RAPIDPoint 500e system uses Win10 IoT Enterprise 1809/LTSC 2019 configured to run in kiosk mode (automatic login and application launch with controls such as key trapper in place to restrict access to the underlying operating system).
Note 16 CSUP-7	Manufacture notify customer of updates
	Release notes are published in Siemens Healthineers Document Library. See https://doclib.siemens-healthineers.com/
Note 17 CSUP-11.1	Customer review of updates
	Release notes for available versions of software are provided in the Siemens Healthineers Document Library. See https://doclib.siemens-healthineers.com/
Note 18 CSUP-11.2	Update review cycle for device
	Third-party components are registered with the Siemens Vulnerability Monitoring service, which notifies users of components when vulnerabilities are identified. Vulnerabilities are tracked as product defects and assessed for criticality. They will either be addressed in a patch release for the product or considered for inclusion when the next product release is commissioned.
Note 19 DTBK-2	Factory Reset function
	A service utility is available to remove data and restore factory settings, but this is not built into the RAPIDPoint 500e system and is only available to service engineers.
Note 20 DTBK-5	Config backup
	System setup can be exported to USB removable media. File containing setup information is encrypted.
Note 21 DTBK-6	Integrity of config backup
	System confirms that setting file is encrypted and can only be opened with the appropriate key.

Note	Note
Note 22	Emergency access
EMRG-1	Field Service can be contacted to obtain a temporary service password (good only for 24 hours) that allows access to the system in the case of emergency.
Note 23	Use of anti-malware software
MLDP-2	MCAFEE Embedded Control (whitelisting solution) is installed on the RAPIDPoint 500e system.
Note 24	Owner reconfigure anti-malware settings
MLDP-2.4	Owner/operator can turn off the anti-malware solution.
Note 25	Repair after malware detection
MLDP2.6	Repair of system after malware detection requires replacement of system hard drive by Field Service engineer.
Note 26	Restrictions on anti-malware
MLDP-2.8	Only McAfee Embedded Control (supplied with the system) is supported.
Note 27	Application whitelisting
MLDP-4	McAfee Embedded Control (whitelisting solution) is installed on the RAPIDPoint 500e system.
Note 28	Network access control mechanisms
NAUT-2	The RAPIDPoint 500e system uses the firewall provided by WINDOWS 10. Further, it allows endpoint identification for LIS and Remote Viewer (VNC) traffic.
Note 29	Firewall ruleset documentation
NAUT-2.1	Information about ports allowed through the firewall is documented in the Product and Solution Security White Paper.
Note 30	USB ports
CONN-1.2.2	The RAPIDPoint 500e system supports USB communication for an integrated bar-code scanner and exposes three USB ports for file transfer. Operating system is configured to prevent auto-launch of executables from the USB media. Setup feature allows power to the USB hub to be turned off (disabling file transfers).
Note 31	Removable memory devices
CON-1.2.3	USB removable memory devices are used for software updates, save/restore of system configuration, and export of data.
Note 32	Other physical connectivity
CONN-1.2.4	The RAPIDPoint 500e system also supports RS- 232 for laboratory information system (LIS) communication and external bar-code scanner input (restricted to Siemens Healthineers-supplied scanner).
Note 33 CONN-2	Ports and protocols are documented in the Product and Solution Security White Paper.
Note 35 CONN-4	The RAPIDPoint 500e system can optionally be configured to transmit email to an SMTP server for transmission of cartridge reliability information to Siemens Healthineers.
Note 36 CONN-7	The RAPIDPoint 500e system supports encrypted LIS communication with the POCcelerator™ Data Management System using TLS 1.2.
Note 37 CONN-8	The RAPIDPoint 500e system supports remote screen view/control via VNC protocol to Siemens Healthineers data managers.
Note 38 PAUT-1, PAUT-1.1	Users are uniquely identifiable, but service access is through a single Service account that does not identify the individual.

Note	Note
Note 39 PAUT-7	The RAPIDPoint 500e system supports operator download from Siemens Healthineers data managers that includes recertification date (and if operator is not renewed by that date, they are prevented from accessing the device).
Note 40 PAUT-8	The system can be configured to require that either the operator ID or password be entered via bar code, while the other is manually entered. Because bar codes can be easily copied, this is not considered true multi-factor authentication.
Note 41 PAUT-10	Operator download from Siemens Healthineers data managers can disable or remove accounts from the RAPIDPoint 500e system.
Note 42 PAUT-14	The RAPIDPoint 500e system stores the operator credentials used to access the device UI. These credentials are valid only on the device (and any other Siemens Healthineers devices in the area if all are controlled by a Siemens Healthineers data manager).
Note 43 RDMP-1	Secure software development process
	Software development is performed following Siemens Healthineers processes, which are modeled after industry standards.
Note 44 RDMP-3	Software support updates information
	Software release notes are published in the Siemens Healthineers Document Library. See https://doclib.siemens-healthineers.com/
Note 45 RDMP-4	Plan for Third Party Component end-of-life
	Third-party components are registered with the Siemens Vulnerability Monitoring service, which includes tracking of end-of-life of components. End-of-life components are considered for replacement as part of future software releases.
Note 46 SBOM-1	SBOM
	Software bill of materials is documented in the Product and Solution Security White Paper.
Note 47 SBOM-2	SBOM standard
	The SBOM is part of the Product and Solution Security White Paper template.
Note 48 SBOM-4	Whenever a new version of the RAPIDPoint 500e system is released, the Product and Solution Security White Paper is updated and rereleased.
Note 49 SAHD-3.2	RAPIDPoint 500e system installation packages are encrypted and confirmed to be valid prior to installation.
Note 50 SAHD-6.1	All RAPIDPoint 500e system user accounts can be reconfigured by the end user. Additionally, the end user can reconfigure the underlying WINDOWS 10 user account (local admin) for both password and account name.
Note 51 SAHD-7	Services needed to support filesharing have been disabled.
Note 52 SAHD-8	Unneeded services, protocols, ports, and applications are disabled/removed as part of master device creation.
Note 53 SAHD-11	Power to USB hub is disabled at power-on until the RAPIDPoint 500e application enables power.
Note 54 SAHD-14.1	Endpoint identification is disabled by default but can be enabled and configured to restrict access to the RAPIDPoint 500e system LIS and VNC protocols to designated IP addresses/subnets.
Note 55 SAHD-16	Auto-launch of executables on removable media has been disabled.
Note 56 SGUD-1	Security features are described in both the RAPIDPoint 500e System Operator’s Guide and in the Product and Solution Security White Paper.

Note	Note
Note 57 STCF-1	The RAPIDPoint 500e system uses WINDOWS 10 Bit-Locker functionality to encrypt the hard drive. The unlock keys are provided by the onboard TPM module, effectively locking the hard drive to the instrument in which it was installed.
Note 58 STCF-3	The RAPIDPoint 500e system uses an embedded database provided by Raima Corporation (RDM V12.0).
Note 59 TXCF-2	While normal LIS communication is unencrypted, the RAPIDPoint 500e system allows connection to the POCcelerator data manager via TLS 1.2 encrypted channel. Facility-viewable patient CSV files exported to removable USB media can optionally be encrypted with a password provided by the facility at the time of data export. Default is encrypted CSV export.
Note 60 TXCF-5, TXIG- 1	The RAPIDPoint 500e system allows connection to the POCcelerator data manager via TLS 1.2 encrypted channel.
Note 61 RMOT-1.2	When a Remote Viewer session to a Siemens Healthineers data manager is active, a button in the banner at the top of the screen indicates that the remote session is active and allows the operator to disconnect the remote viewing session. Note: This is a remote viewing session within the facility environment (not from Siemens Healthineers).

Abbreviations

AD	Active Directory
ADT	Admission, Discharge, Transfer
AES	Advanced Encryption Standard
AMD	Advanced Micro Devices, Inc
BIOS	Basic Input Output System
CERT	Computer Emergency Readiness Team
CSV	Comma Separated Values
DES	Data Encryption Standard
DISA	Defense Information Systems Agency
DMZ	Demilitarized Zone
DoS	Denial of Service
ePHI	Electronic Protected Health Information
FDA	Food and Drug Administration
FIFO	First-in, First-out
FIPS	Federal Information Processing Standards
FPGA	Field Programmable Gate Array
HHS	Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HIMSS	Healthcare Information and Management Systems Society
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
ICMP	Internet Control Message Protocol
IEC	International Electrotechnical Commission
IoT	Internet of Things
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
LIS	Laboratory Information System
LLMNR	Link-Local Multicast Name Resolution
LTSC	Long Term Service Channel
MD5	Message Digest 5
MDS2	Manufacturer Disclosure Statement for Medical Device Security
NEMA	National Electrical Manufacturers Association
NTP	Network Time Protocol
OCR	Office for Civil Rights
OS	Operating System
PEP	Personalized Education Plan
PHI	Protected Health Information
PII	Personally Identifiable Information
POC	Point of Care
RDM	Raima Data Manager
RPC	Remote Procedure Call
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
SRS	Smart Remote Services
SSL	Secure Sockets Layer
STAPL	Standard Test And Programming Language
SW	Software
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TPM	Trusted Platform Module
UDP	User Datagram Protocol
USB	Universal Serial Bus
VNC	Virtual Network Computing
VPN	Virtual Private Network

Disclaimer according to IEC 80001-1

1-1 The Device has the capability to be connected to a medical IT-network which is managed under full responsibility of the operating responsible organization. It is assumed that the responsible organization assigns a Medical IT-Network Risk Manager to perform IT-Risk Management (see IEC 80001-1:2010/EN 80001-1:2011) for IT-networks incorporating medical devices.

1-2 This statement describes Device-specific ITnetworking safety and security capabilities. It is not a responsibility agreement according to IEC 80001-1:2010/EN 80001-1:2011.

1-3 Any modification of the platform, the software or the interfaces of the Device—unless authorized and approved by Siemens Healthcare GmbH Healthcare—voids all warranties, liabilities, assertions and contracts.

1-4 The responsible organization acknowledges that the Device's underlying standard computer with operating system is to some extent vulnerable to typical attacks like e.g. malware or denial-of-service.

1-5 Unintended consequences (like e.g. misuse/loss/corruption) of data not under control of the Device e.g. after electronic communication from the Device to some IT-network or to some storage, are under the responsibility of the responsible organization.

1-6 Unauthorized use of the external connections or storage media of the Device can cause hazards regarding the availability and information security of all components of the medical IT-network. The responsible organization must ensure—through technical and/or organizational measures—that only authorized use of the external connections and storage media is permitted.

International Electrotechnical Commission Glossary (extract)

Responsible organization: Entity accountable for the use and maintenance of a medical IT-network.

Statement on FDA Cybersecurity Guidance

Siemens Healthineers will follow cybersecurity guidance issued by the FDA as appropriate. Siemens Healthineers recognizes the principle described in FDA cybersecurity guidance that an effective cybersecurity framework is a shared responsibility among multiple stakeholders (e.g., medical device manufacturers, healthcare facilities, patients, and providers) and is committed to drawing on its innovation, engineering, and pioneering skills in collective efforts designed to prevent, detect, and respond to new and emerging cybersecurity threats. While FDA cybersecurity guidance is informative as to adopting a risk-based approach to addressing potential patient harm, it is not binding, and alternative approaches may be used to satisfy FDA regulatory requirements.

The representations contained in this white paper are designed to describe Siemens Healthineers approach to cybersecurity of its medical devices and to disclose the security capabilities of the devices/systems described herein. Neither Siemens Healthineers nor any medical device manufacturer can warrant that its systems will be invulnerable to cyberattack. Siemens Healthineers makes no representation or warranty that its cybersecurity efforts will ensure that its medical devices/systems will be error-free or secure against cyberattack.

At Siemens Healthineers, our purpose is to enable healthcare providers to increase value by empowering them on their journey toward expanding precision medicine, transforming care delivery, and improving patient experience, all made possible by digitalizing healthcare.

An estimated 5 million patients globally benefit every day from our innovative technologies and services in the areas of diagnostic and therapeutic imaging, laboratory diagnostics, and molecular medicine, as well as digital health and enterprise services.

We are a leading medical technology company with over 120 years of experience and 18,000 patents globally. Through the dedication of more than 50,000 colleagues in 75 countries, we will continue to innovate and shape the future of healthcare.

Product availability may vary from country to country and is subject to varying regulatory requirements. Please contact your local representative for availability.

Siemens Healthineers Headquarters
Siemens Healthcare GmbH
Henkestr. 127
91052 Erlangen, Germany
Phone: +49 9131 84-0
siemens-healthineers.com

Published by
Siemens Healthcare Diagnostics Inc.
Point of Care Diagnostics
2 Edgewater Drive
Norwood, MA 02062-4637
USA
Phone: +1 781-269-3000

Published by Siemens Healthcare Diagnostics Inc. · Order No. 40-21-DX-587-76 · 05-2021 · ©Siemens Healthcare Diagnostics Inc., 2021