Security White Paper and MDS² Form

RAPIDPoint 500e Blood Gas Systems V5.0

The facts about the security of our products and solutions

siemens-healthineers.com/rapidpoint500e

Not available for sale in the U.S. Product availability varies from country to country.

SIEMENS Healthineers

Contents

Foreword

The Siemens Healthineers product and solution security 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 of our medical devices.

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

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 in and incidents involving our medical devices, 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 medical devices
- Incorporating secure architecture, design, and coding methodologies in our software development process
- Performing static code analysis of medical device software
- Conducting security testing of medical devices under development as well as medical devices 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 components issues in our medical devices
- Working with suppliers to address security throughout the supply chain
- Training 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

For all other communication with Siemens Healthineers about product and solution security: ProductTechnologyAssurance.dl@siemens-healthineers.com.

Jim Jacobson
Chief Product and Solution Security Officer
Siemens Healthineers

Elevate Your Blood Gas Solution

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.

Use of encryption
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 network message traffic using TLS 1.2.

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), FI02, 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 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.

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.

Network Information

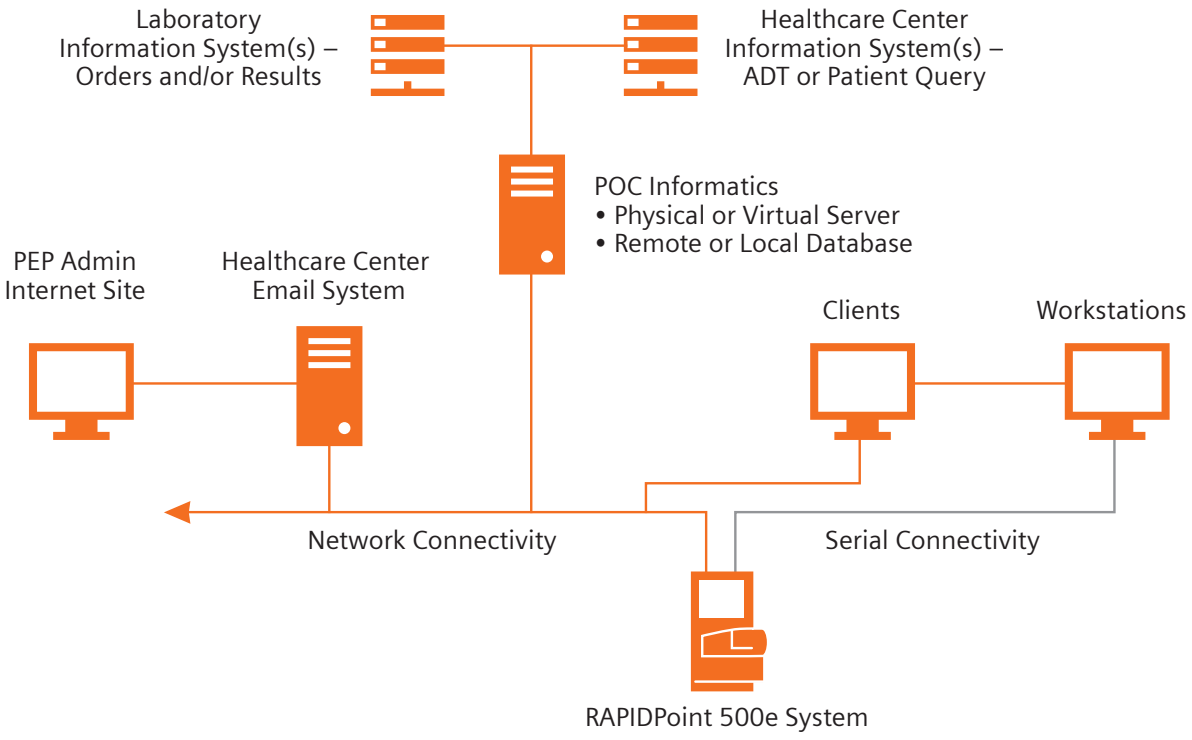

Table 1. The server requires no static IP addresses, but may be configured in static IP address mode if desired by the facility. The following ports are used by the system:

Port Number	Service/Function	Direction	Protocol
25	SMTP email (optional)	Outbound	SMTP
3001	LIS communication with data manager (port number is user configurable)	Inbound	LIS3/LIS4
5900	Remote Viewer	Inbound	VNC

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 authorization controls
- 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.

Continuous vulnerability assessment and remediation
- 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
- System 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 a ccess 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 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 protection
- RAPIDPoint 500e instrument should reside and be operated in a physically controlled environment.
- P/S2 keyboard port is not exposed.
- USB hub is not powered until instrument application is running.
- USB hub power can be configured by System Supervisor as off except for Level 1 operations such as Save/Restore Setup and Software Installation.

Auditing/logging
Event logging tracks some key user activities.

Remote connectivity
- Connection to external data manager is available via TCP connection (on port 3001 by default, configurable by facility). Connection to POCcelerator™ Data Management System can be encrypted using 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).

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.

Table 2. The most relevant third-party technologies used.

Vendor Name	Component Name	Component Version	Description/Use
MICROSOFT	WINDOWS IoT Enterprise Version 1809	10	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	Compression with encryption
Tight VNC	VNC Server	2.7.10	Remote Viewer
TouchBase	Universal Pointing Device Driver	3.05.18	Touchscreen utilities
Motorola	SNAPI.dll	3.0.0.5	USB bar-code reader interface library
OpenSSL.org	OpenSSL	1.1.0k	TLS 1.2 encryption of network LIS traffic

Manufacturer Disclosure Statement according to IEC60601-1

Table 3. Statement according to IEC 60601-1, 3rd Edition, Chapter 14.13.

1	Network properties required by the system and resulting risks
1-1	RAPIDPoint 500e system does NOT need access to the internet to function. As such, it should be deployed on a limited access (nonpublic) network.
1-2	If the analyzer uses email to send log files to Siemens Healthineers, the gateway must be configured to allow the data to be sent to the SMTP server.
2	**Instructions for the responsible organization**
2-1	RAPIDPoint 500e system should reside and be operated in a physically controlled environment.
2-2	Default System Supervisor password should be changed to a local site-specific value after installation.

HN 1-2013

Manufacturer Disclosure Statement for Medical Device Security – MDS²

DEVICE DESCRIPTION

Device Category	Manufacturer	Document ID	Document Release Date
	Siemens Healthineers	DX014286 Rev 01	

Device Model	Software Revision	Software Release Date
RAPIDPoint 500e System	V5.0	25 Jul 2019

Manufacturer or Representative Contact Information	Company Name	Manufacturer Contact Information
	Siemens Healthineers	
	Representative Name/Position	

Intended use of **device** in network-connected environment:

Transmission of Results/Status with LIS/DataManager System
Email for Cartridge Credit

MANAGEMENT OF PRIVATE DATA

	Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #
A	Can this **device** display, transmit, or maintain **private data** (including **electronic Protected Health Information** [ePHI])?	Yes	
B	Types of **private data** elements that can be maintained by the **device**:		
B.1	Demographic (e.g., name, address, location, unique identification number)?	Yes	
B.2	Medical record (e.g., medical record #, account #, test or treatment date, **device** identification number)?	Yes	
B.3	Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)?	Yes	
B.4	Open, unstructured text entered by **device user/operator**?	See Note	1
B.5	**Biometric data**?	No	
B.6	Personal financial information?	No	
C	Maintaining **private data** - Can the **device**:		
C.1	Maintain **private data** temporarily in volatile memory (i.e., until cleared by power-off or reset)?	Yes	
C.2	Store **private data** persistently on local media?	Yes	
C.3	Import/export **private data** with other systems?	Yes	
C.4	Maintain **private data** during power service interruptions?	Yes	
D	Mechanisms used for the transmitting, importing/exporting of **private data** – Can the **device**:		
D.1	Display private data (e.g., video display, etc.)?	Yes	
D.2	Generate hardcopy reports or images containing **private data**?	Yes	
D.3	Retrieve **private data** from or record **private data** to **removable media** (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick, etc.)?	Yes	
D.4	Transmit/receive or import/export **private data** via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire, etc.)?	Yes	
D.5	Transmit/receive **private data** via a wired network connection (e.g., LAN, WAN, VPN, intranet, Internet, etc.)?	Yes	
D.6	Transmit/receive **private data** via an integrated wireless network connection (e.g., WiFi, Bluetooth, infrared, etc.)?	No	
D.7	Import **private data** via scanning?	Yes	
D.8	Other?	N/A	

1. Limited to 15 Characters for Custom Demographics fields.

Management of Private Data notes:

HN 1-2013

Device Category	Manufacturer	Document ID	Document Release Date
	Siemens Healthineers	DX014286 Rev 01	
Device Model	**Software Revision**		**Software Release Date**
RAPIDPoint 500e System	V5.0		25 Jul 2019

SECURITY CAPABILITIES

	Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #
1	**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.		
1-1	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)?	No	
	1-1.1 Is the length of inactivity time before auto-logoff/screen lock **user** or administrator configurable? (Indicate time [fixed or configurable range] in notes.)	N/A	
	1-1.2 Can auto-logoff/screen lock be manually invoked (e.g., via a shortcut key or proximity sensor, etc.) by the **user**?	N/A	
ALOF notes:			
2	**AUDIT CONTROLS (AUDT)**		
	The ability to reliably audit activity on the **device**.		
2-1	Can the **medical device** create an **audit trail**?	No	
2-2	Indicate which of the following events are recorded in the audit log:		
	2-2.1 Login/logout	See Note	2
	2-2.2 Display/presentation of data	No	
	2-2.3 Creation/modification/deletion of data	No	
	2-2.4 Import/export of data from **removable media**	No	
	2-2.5 Receipt/transmission of data from/to external (e.g., network) connection	No	
	2-2.5.1 **Remote service** activity	N/A	
	2-2.6 Other events? (describe in the notes section)	N/A	
2-3	Indicate what information is used to identify individual events recorded in the audit log:		
	2-3.1 **User** ID	No	
	2-3.2 Date/time	Yes	
	2. Successful logins are recorded in the audit log.		
AUDT notes:			
3	**AUTHORIZATION (AUTH)**		
	The ability of the device to determine the authorization of users.		
3-1	Can the **device** prevent access to unauthorized **users** through **user** login requirements or other mechanism?	See Note	3
3-2	Can **users** be assigned different privilege levels within an application based on 'roles' (e.g., guests, regular **users**, power **users**, administrators, etc.)?	Yes	
3-3	Can the **device** owner/**operator** obtain unrestricted administrative privileges (e.g., access operating system or application via local root or admin account)?	No	
AUTH notes:	3. When the system is set to "Restricted" mode, it prompts for user login to access the system. When the system is in "Limited" mode, it prompts for user login for select screens such as Cart Replacement, Calibrations, Setup, etc.		

HN 1-2013

Device Category	Manufacturer	Document ID	Document Release Date
	Siemens Healthineers	DX014286 Rev 01	
Device Model	**Software Revision**		**Software Release Date**
RAPIDPoint 500e System	V5.0		25 Jul 2019

	Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #
4	**CONFIGURATION OF SECURITY FEATURES (CNFS)**		
	The ability to configure/re-configure **device security capabilities** to meet **users'** needs.		
4-1	Can the **device** owner/operator reconfigure product **security capabilities**?	See Note	4
CNFS notes:	4. User can reconfigure security features of the application only. User cannot install additional security capabilites.		
5	**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.		
5-1	Can relevant OS and **device** security patches be applied to the **device** as they become available?	See Note	5
5-1.1	Can security patches or other software be installed remotely?	No	__
CSUP notes:	5. Security patches are included as part of Siemens Healthineers software release media, but are not installable without the software release (i.e., no operating system-specific patches).		
6	**HEALTH DATA DE-IDENTIFICATION (DIDT)**		
	The ability of the **device** to directly remove information that allows identification of a person.		
6-1	Does the **device** provide an integral capability to de-identify **private data**?	See Note	6
DIDT notes:	6. Field Service has access to a tool that can remove PHI from the database.		
7	**DATA BACKUP AND DISASTER RECOVERY (DTBK)**		
	The ability to recover after damage or destruction of **device** data, hardware, or software.		
7-1	Does the **device** have an integral data backup capability (i.e., backup to remote storage or **removable media** such as tape, disk)?	See Note	7
DTBK notes:	7. Yes, the user can back up data to comma-separated value (csv) data files with patient results including ePHI. No data run-time restore.		
8	**EMERGENCY ACCESS (EMRG)**		
	The ability of **device users** to access **private data** in case of an emergency situation that requires immediate access to stored **private data**.		
8-1	Does the **device** incorporate an **emergency access** ("break-glass") feature?	Yes	8
EMRG notes:	8. Password of the day provided by Siemens Healthineers Support.		
9	**HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU)**		
	How the **device** ensures that data processed by the **device** has not been altered or destroyed in an unauthorized manner and is from the originator.		
9-1	Does the **device** ensure the integrity of stored data with implicit or explicit error detection/correction technology?	No	__
IGAU notes:			

HN 1-2013

Device Category	Manufacturer	Document ID	Document Release Date
	Siemens Healthineers	DX014286 Rev 01	
Device Model	**Software Revision**		**Software Release Date**
RAPIDPoint 500e System	V5.0		25 Jul 2019

	Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #
10	**MALWARE DETECTION/PROTECTION (MLDP)**		
	The ability of the **device** to effectively prevent, detect and remove malicious software (**malware**).		
10-1	Does the **device** support the use of **anti-malware** software (or other **anti-malware** mechanism)?	Yes	__
	10-1.1 Can the **user** independently re-configure **anti-malware** settings?	Yes	__
	10-1.2 Does notification of **malware** detection occur in the **device user** interface?	No	__
	10-1.3 Can only manufacturer-authorized persons repair systems when **malware** has been detected?	Yes	__
10-2	Can the device owner install or update **anti-virus software**?	No	__
10-3	Can the device owner/**operator** (technically/physically) update virus definitions on manufacturer-installed **anti-virus software**?	No	__
MLDP notes:			
11	**NODE AUTHENTICATION (NAUT)**		
	The ability of the **device** to authenticate communication partners/nodes.		
11-1	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?	Yes	11
NAUT notes:	11. Firewall endpoint can be configured to accept only authorized nodes.		
12	**PERSON AUTHENTICATION (PAUT)**		
	Ability of the **device** to authenticate **users**		
12-1	Does the **device** support **user/operator**-specific username(s) and password(s) for at least one **user**?	Yes	
	12-1.1 Does the device support unique **user/operator**-specific IDs and passwords for multiple users?	Yes	__
12-2	Can the **device** be configured to authenticate **users** through an external authentication service (e.g., MS Active Directory, NDS, LDAP, etc.)?	No	__
12-3	Can the **device** be configured to lock out a **user** after a certain number of unsuccessful logon attempts?	No	__
12-4	Can default passwords be changed at/prior to installation?	Yes	
12-5	Are any shared **user** IDs used in this system?	No	__
12-6	Can the **device** be configured to enforce creation of **user** account passwords that meet established complexity rules?	No	__
12-7	Can the **device** be configured so that account passwords expire periodically?	Yes	
PAUT notes:	12-1 The device prompts for a password and recognizes the user based on the password entered. It does not prompt for both username and password for one-step authentication. For two-step authentication, both operator and password are displayed, but this is not the default setup. 12-7 Yes, passwords expire when used with the RAPIDComm® Data Management System.		
13	**PHYSICAL LOCKS (PLOK)**		
	Physical locks can prevent unauthorized **users** with physical access to the **device** from compromising the integrity and confidentiality of **private data** stored on the **device** or on **removable media**.		
13-1	Are all **device** components maintaining **private data** (other than **removable media**) physically secure (i.e., cannot remove without tools)?	Yes	__
PLOK notes:			

HN 1-2013

Device Category	Manufacturer	Document ID	Document Release Date
	Siemens Healthineers	DX014286 Rev 01	
Device Model	**Software Revision**		**Software Release Date**
RAPIDPoint 500e System	V5.0		25 Jul 2019

	Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #
14	**ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP)**		
	Manufacturer's plans for security support of 3rd party components within **device** life cycle.		
14-1	In the notes section, list the provided or required (separately purchased and/or delivered) operating system(s) - including version number(s).	See Note	14.1
14-2	Is a list of other third party applications provided by the manufacturer available?	Yes	2
RDMP notes:	14-1 WINDOWS 10 IoT Enterprise plus subsequent application updates. 14-2 Most third-party software used is referenced in RAPIDPoint 500e Release Notes. In addition, we use a Raima database and MCAFEE anti-virus software.		
15	**SYSTEM AND APPLICATION HARDENING (SAHD)**		
	The **device**'s resistance to cyber attacks and **malware**.		
15-1	Does the **device** employ any hardening measures? Please indicate in the notes the level of conformance to any industry-recognized hardening standards.	Yes	15.1
15-2	Does the **device** employ any mechanism (e.g., release-specific hash key, checksums, etc.) to ensure the installed program/update is the manufacturer-authorized program or software update?	Yes	
15-3	Does the **device** have external communication capability (e.g., network, modem, etc.)?	See Note	3
15-4	Does the file system allow the implementation of file-level access controls (e.g., New Technology File System (NTFS) for MS Windows platforms)?	No	
15-5	Are all accounts which are not required for the **intended use** of the **device** disabled or deleted, for both **users** and applications?	Yes	
15-6	Are all shared resources (e.g., file shares) which are not required for the **intended use** of the **device**, disabled?	Yes	
15-7	Are all communication ports which are not required for the **intended use** of the **device** closed/disabled?	Yes	
15-8	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	
15-9	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	
15-10	Can the **device** boot from uncontrolled or **removable media** (i.e., a source other than an internal drive or memory component)?	No	
15-11	Can software or hardware not authorized by the **device** manufacturer be installed on the device without the use of tools?	No	
SAHD notes:	15-1 Uses embedded version of operating system with fewer components, prevents auto-launch. 15-3 The device can be connected to a LAN (for connection to external data manager) but does not connect to internet.		
16	**SECURITY GUIDANCE (SGUD)**		
	The availability of security guidance for **operator** and administrator of the system and manufacturer sales and service.		
16-1	Are security-related features documented for the **device user**?	Yes	
16-2	Are instructions available for **device**/media sanitization (i.e., instructions for how to achieve the permanent deletion of personal or other sensitive data)?	Yes	16.2
	16-2 Available to Service but not to users.		
SGUD notes:			

HN 1-2013

Device Category	Manufacturer	Document ID	Document Release Date
	Siemens Healthineers	DX014286 Rev 01	
Device Model	**Software Revision**		**Software Release Date**
RAPIDPoint 500e System	V5.0		25 Jul 2019

		Yes, No, N/A, or See Note	Note #
	Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.		
17	**HEALTH DATA STORAGE CONFIDENTIALITY (STCF)**		
	The ability of the **device** to ensure unauthorized access does not compromise the integrity and confidentiality of **private data** stored on **device** or **removable media**.		
17-1	Can the **device** encrypt data at rest?	Yes	__
STCF notes:			
18	**TRANSMISSION CONFIDENTIALITY (TXCF)**		
	The ability of the **device** to ensure the confidentiality of transmitted **private data**.		
18-1	Can **private data** be transmitted only via a point-to-point dedicated cable?	No	__
18-2	Is **private data** encrypted prior to transmission via a network or **removable media**? (If yes, indicate in the notes which encryption standard is implemented.)	Yes	18
18-3	Is **private data** transmission restricted to a fixed list of network destinations?	Yes	__
TXCF notes:	18-1 Uses TLS 1.2 for network LIS encryption.		
19	**TRANSMISSION INTEGRITY (TXIG)**		
	The ability of the **device** to ensure the integrity of transmitted **private data**.		
19-1	Does the **device** support any mechanism intended to ensure data is not modified during transmission? (If yes, describe in the notes section how this is achieved.)	Yes	19-1
TXIG notes:	19-1 Uses checksum		
20	**OTHER SECURITY CONSIDERATIONS (OTHR)**		
	Additional security considerations/notes regarding **medical device** security.		
20-1	Can the **device** be serviced remotely?	No	__
20-2	Can the **device** restrict remote access to/from specified devices or **users** or network locations (e.g., specific IP addresses)?	No	__
	20-2.1 Can the **device** be configured to require the local **user** to accept or initiate remote access?	Yes	2
	20-2 Remote access can be enabled/disabled by local user. Local user can see Remote Viewer		
OTHR notes:			

Abbreviations

AD	Active Directory
AES	Advanced Encryption Standard
AMD	Advanced Micro Devices, Inc.
BIOS	Basic Input Output System
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
FIPS	Federal Information Processing Standards
HHS	Health and Human Services
HIMSS	Healthcare Information and Management Systems Society
HIPAA	Health Insurance Portability and Accountability Act
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
ICS	Integrated Communication Services
IEC	International Electrotechnical Commission
IoT	Internet of Things
LDAP	Lightweight Directory Access Protocol
MD5	Message Digest 5
MDS2	Manufacturer Disclosure Statement
MSTS	Microsoft Terminal Server
NEMA	National Electrical Manufacturers Association
NTP	Network Time Protocol
OCR	Office for Civil Rights
OU	Organizational Unit
PHI	Protected Health Information
PII	Personally Identifiable Information
RPC	Remote Procedure Call
SAM	Security Accounts Manager
SHA	Secure Hash Algorithm
SQL	Structured Query Language
SRS	Siemens Remote Service
SSL	Secure Sockets Layer
SW	Software
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TPM	Trusted Platform Module
Ultra-VNC	Ultra Virtual Network Computing
UDP	User Datagram Protocol
VPN	Virtual Private Network

International Electrotechnical Commission
Glossary (extract) Responsible organization:
Entity accountable for the use and maintenance of a medical IT-network.

Disclaimer According to IEC 80001-1

1-1 The Device has the capability to be connected to a medical IT network that 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 IT-networking 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–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, such as e.g., malware or denial-of-service.

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

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.

Not available for sale in the U.S. 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. 40-19-14019-01-76 · 12-2019 · ©Siemens Healthcare Diagnostics Inc., 2019