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. 40-20-14270-01-76 · 08-2020 · ©Siemens Healthcare Diagnostics Inc., 2020

Version 3.32 and Higher Security White Paper and MDS^2 Form

epoc Blood Analysis System

The facts about the security of our products and solutions

siemens-healthineers.com/epoc

SIEMENS
Healthineers

Contents

Basic Information 4

Network Information 6

Security Controls 7

Software Bill of Materials 8

Manufacturer Disclosure Statement (IEC 60601-1) 9

Manufacturer Disclosure Statement (MDS²) 10–16

Abbreviations 17

Disclaimer According to IEC 80001-1 17

Statement on FDA Cybersecurity Guidance 17

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

Basic Information

The epoc® Blood Analysis System is a portable point-of-care blood analyzer used for quantitative in vitro diagnostic testing of whole blood samples. The epoc system is intended to be used by trained medical professionals at a patient's bedside or in a laboratory or other clinical environment. The following are some of the epoc system's primary features:

- The epoc system delivers results for a full menu of lab-accurate tests using fresh whole blood at the patient's bedside in less than 1 minute after sample introduction.
- The epoc system can be customized to support various workflows in different clinical environments.
- The epoc system is wireless and can easily integrate with the epoc Enterprise Data Manager and other supported third-party data managers to centrally manage devices and patient results across the entire institution when interfaced with the facility's LIS/HIS/EMR.

The epoc Blood Analysis System consists of the following components:

- **epoc Reader:** The epoc Reader is a portable, battery-powered device that, when used in conjunction with the epoc Host and Test Card, performs the amplifying, digitizing, and conversion of raw sensor signals to produce blood test results.
- **epoc Host:** The epoc Host is a handheld mobile computer designed to work with the epoc Reader. The epoc Host runs specialized, user-friendly, highly configurable software that guides users through the testing process and can connect to a facility's existing wireless network to synchronize with a supported data-management system. Healthcare personnel can receive, review, and document results immediately while at the patient's bedside in addition to making those results available in real time to the entire care team.
- **epoc Test Card:** The epoc Test Cards are single-use, individually wrapped, room temperature-stable devices used in conjunction with the epoc Reader and Host to produce blood test results. The Test Card contains electrochemical sensors, calibration fluid, and fluidic channels to accurately measure blood gases, a basic metabolic panel (BMP), hematocrit, and lactate concentrations from arterial, venous, or capillary whole-blood samples.
- **Accessories:** epoc Care-Fill™ capillary tubes, aqueous QC and calibration/verification fluids, portable printer(s), epoc Enterprise Data Manager (EDM), eDM Lite.

Operating systems

- epoc Host²: MICROSOFT WINDOWS Embedded Handheld 6.5
- epoc Reader: no operating system installed

Hardware specifications

epoc Host²:

- Manufacturer: ZEBRA Technologies
- Model: MC55A0 or MC55E0
- CPU:
  - (MC55A0) MARVELL PXA320 Processor @ 806 MHz
  - (MC55E0) Dual Core @ 800 MHz OMAP 4 processor
- Memory:
  - (MC55A0) 256 MB RAM, 1 GB flash
  - (MC55E0) 512 MB RAM, 1 GB flash
- WLAN:
  - (MC55A0) Tri-mode IEEE 802.11a/b/g (2.4/5 GHz)
  - (MC55E0) Quad-mode IEEE 802.11a/b/g/n (2.4/5 GHz)
- BLUETOOTH:
  - (MC55A0) BCM2046 BT Module Class II v2.1 (EDR)
  - (MC55E0) TI WiLink 7.0 BT Module Class II v2.1 (EDR)
- microSD slot (maximum 32 GB)
- Display: 3.5 in. color VGA, super-bright 650+ NITS (glass analog resistive touch screen)
- Bar-code:
  - (MC55A0) Integrated Zebra SE4500-DL 1D/2D bar-code imager
  - (MC55E0) Integrated Zebra SE4710 1D/2D bar-code imager
- Rechargeable lithium ion 3.7 V, 3600 mAh battery
- Numeric keypad
- Sealing: IP64
- Drop: Multiple 6 ft/1.8 m drops per MIL-STD 810G

epoc Reader

- Manufacturer: Siemens Healthcare Diagnostics Inc.
- CPU: Microchip ARM-based SAM7S256 @ 55 MHz
- ULTRALIFE lithium ion rechargeable battery
- BLUETOOTH: Class II v2.1 EDR
- BLUETOOTH Module: EZURIO BISM2 or BISMS02BI-01

User account information

- The epoc Host supports two user types: Host Administrator and Host Operators.
- The Host Administrator is authorized to:
  - Access the operating system
  - Configure the device
  - Manage Host Operators
  - Update device software
  - View, print, and delete stored tests
- Host Operators (up to 4000) can be managed directly on the device or on a supported data manager.
- Host Operators can be authorized to:
  - Run patient tests
  - Run QA tests
  - Update device software
  - View and print stored tests

Patching strategy

- Siemens Healthineers releases software for the epoc Blood Analysis System twice yearly. These updates include application updates and, if available, appropriate operating system updates.
- Siemens Healthineers does not support installing any nonapproved software on this medical device beyond the software releases provided by Siemens Healthineers.

Cryptography usage

Data stored on the epoc Reader:

- The epoc Reader measures and stores raw sensor waveforms from each epoc BGEM Test Card.
- Data stored on the epoc Reader does not contain Protected Health Information and is not encrypted.

Data stored on the epoc Host²:

- The epoc Host² stores test records that consist of patient and QA test results, patient demographics, operator-entered parameters, operator information, and other related miscellaneous data.
- The epoc Host² stores test records containing PHI using triple-DES encryption with 192-bit key pair generation.

Data transmitted between the epoc Host and Reader:

- Data is transmitted between the epoc Reader and epoc Host² using BLUETOOTH 2.1 EDR and is encrypted using BLUETOOTH standard 128-bit encryption with PIN authentication.
- Data transmitted between the epoc Reader and epoc Host² includes raw measurement and QA data and does not contain PHI.

Data transmitted between the epoc Host and Data Manager:

- Patient test records can be transmitted from the epoc Host² to a supported data manager via the facility's existing wireless LAN (WLAN).
- WLAN connections are managed using ZEBRA Wireless Fusion device software.
- ZEBRA Wireless Fusion is FIPS 140-2–certified (ref. NIST FIPS 140-2 Validation Certificate #2328) and supports industry-standard security protocols including WPA2 (AES) Personal and WPA2 (AES) Enterprise and various EAP methods.
- Wi-Fi security support: WEP (40/128), WPA (TKIP), WPA2 (AES), TLS, TTLS (MS-CHAP), TLS (MS-CHAP v2), TTLS (CHAP), TTLS-MD5, TTLS-PAP, PEAP-TLS, PEAP (MS-CHAP v2), LEAP, FAST
- Wi-Fi certification: CCXv4-certified, FIPS 140-2–certified (NIST FIPS 140-2 Certificate #2328)

Handling of sensitive data

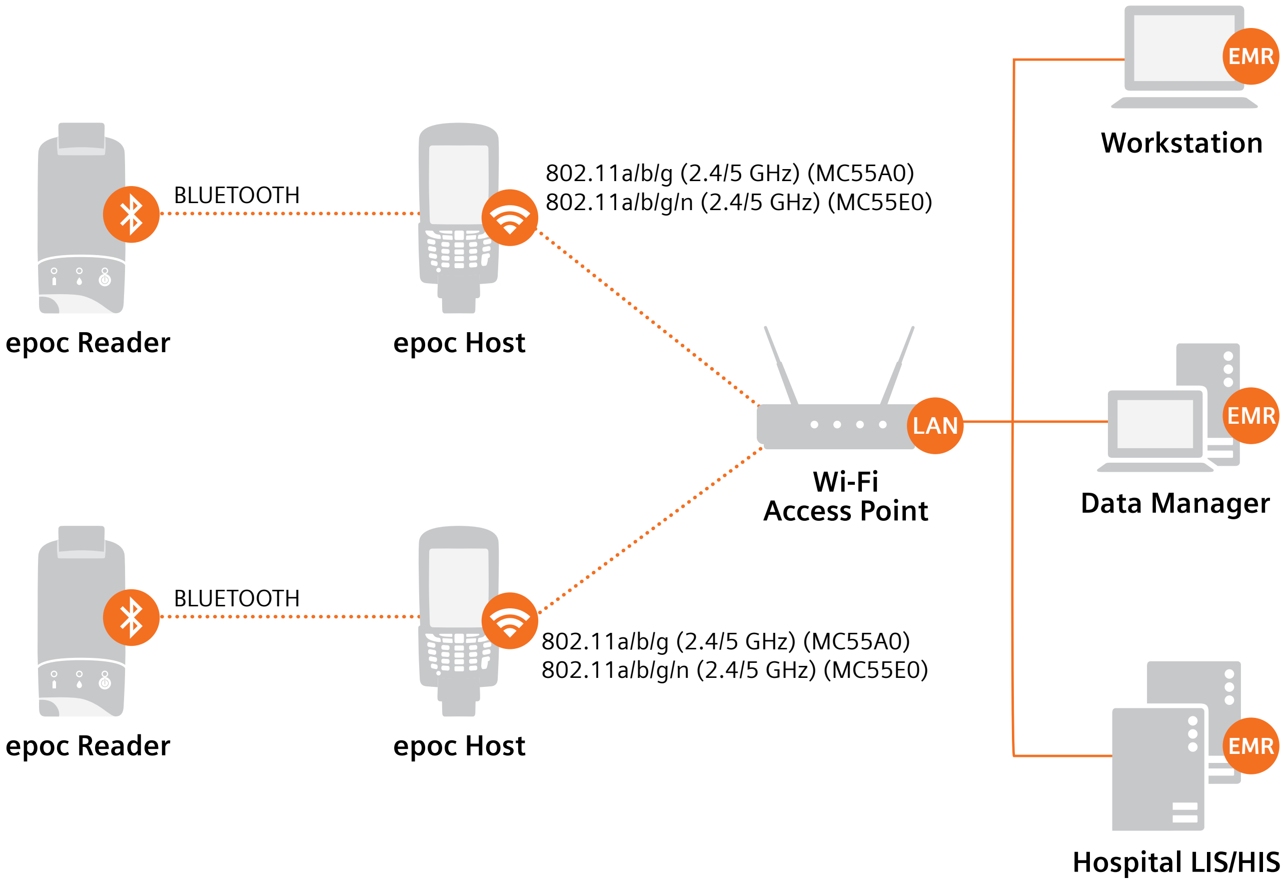
epoc Reader:

- Data stored on the epoc Reader does not contain PHI.
- The epoc Reader measures and stores raw sensor waveforms from each epoc BGEM Test Card and transmits the raw waveforms to the epoc Host² using BLUETOOTH 2.1 EDR.
- For the purposes of troubleshooting, the epoc Reader will store the last 20 electronic QC results as well as QC and calibration verification results.

Sensitive data stored on the epoc Host:

- The epoc Host stores the last 2000 patient and QA test records and purges these records in first-in, first-out (FIFO) order.
- Authorized Host Operators can view and print stored test records.
- The Host Administrator may view, print, and delete one or more stored test records.
- Patient and sample demographic data can be entered by the operator via on-screen data entry.
- Test records may consist of the following data:
  - Patient demographics, including a patient ID (e.g., account #, medical record #, etc.), first name, last name, gender, and date of birth. Patient demographic data is user-entered or retrieved from a supported data-management system based on matching patient ID.
  - Operator information, including operator ID, operator name, and certification expiration
  - Operator-entered information, such as location, physician ID, accession number, operator ID, temperature, FiO^2, flow, respiratory rate, barometric pressure, CPAP, PEEP, PIP, tidal volume, Allen test, and free-text comments
  - Patient and QA test results
  - Other miscellaneous data, including application logs and raw diagnostic data received from the epoc Reader for analysis.
- Raw diagnostic files and logs may be requested by Siemens Healthineers during troubleshooting events. These can be retrieved from supported data-management systems. PHI is not present in the raw diagnostic files.

Network Information


epoc Reader
BLUETOOTH
epoc Host
802.11a/b/g (2.4/5 GHz) (MC55A0)
802.11a/b/g/n (2.4/5 GHz) (MC55E0)
Workstation
EMR
LAN
Wi-Fi Access Point
Data Manager
EMR
epoc Reader
BLUETOOTH
epoc Host
802.11a/b/g (2.4/5 GHz) (MC55A0)
802.11a/b/g/n (2.4/5 GHz) (MC55E0)
Hospital LIS/HIS
EMR

If the epoc system will be connected to a supported data manager, each WLAN-connected epoc Host[2] requires one DHCP-assigned IP address, which must be provided by the customer. The following ports may be used by the system:

Port number	Service/Function	Direction	Protocol
Configurable	Synchronization with a supported data manager	Bidirectional	Proprietary

Security Controls

Malware protection

- The epoc Host does not support anti-virus or anti-malware software.
- The epoc Reader operates on custom firmware that cannot be modified by malware.
- Controlled use of administrative privileges
- The system distinguishes between clinical and administrative roles. Clinical users are Host Operators and do not require administrative privileges. Authorization as Host Administrator is required for administrative tasks.
- Administrator account is protected by a configurable password.
- The epoc Host runs in kiosk mode, preventing Host Operator access to the operating system. Only the Host Administrator is authorized to access the operating system.

Authentication authorization controls

- The epoc Host supports two user types with different permissions: one Host Administrator and 4000 unique Host Operators.
- Host Operator access can be configured to require ID only or ID and password to run and view tests.
- Supports use of strong passwords that may contain:
  – Four to 20 characters in length
  – One or more uppercase characters
  – One or more lowercase characters
  – One or more numeric characters (0–9)
  – One or more special characters
- The system may be configured to log out automatically after a configurable period of inactivity.
- The system is configured to lock itself after five incorrect log-in attempts.
- Continuous vulnerability assessment and remediation
- All third-party components are registered with Siemens Vulnerability Monitoring and are reviewed and monitored for vulnerabilities that may affect the product.

Hardening

- The epoc system is designed as a closed system that allows only the Host Administrator to access the operating system.
- The epoc System is configured to run in kiosk mode to prevent Host Operators from accessing the underlying operating system.
- Unnecessary ports and services can be disabled.
- Auto-launch of executables when removable media is inserted has been disabled.

Network controls

- Network controls are at the discretion of each facility's processes and procedures. The epoc system is designed to effectively integrate into facilities' networks using industry-standard WLAN technology.
- Supports MAC address filtering.
- Supports security certificates.
- Internet access is not needed to operate the device.
- Siemens Healthineers recommends operating the system in a secured network environment, e.g., a separate network segment or a VLAN. An unprotected connection to the internet is discouraged.
- In case of a denial of service (DoS) or malware attack, the system can be taken off the network and operated as a stand-alone device.

Physical protection

- The epoc system does not include any physical protection mechanisms.
- The customer is responsible for tracking and protecting the device.

Data protection controls

- The epoc Host maintains the last 2000 patient and QC records, which are encrypted on the device.
- The epoc Host can export patient results, QC results, and other corresponding data to a supported data-management system.

Auditing/logging

Device application logs track system and user activities.

Remote connectivity

The epoc Blood Analysis System does not support remote connections.

Administrative controls

Certain features are accessible only to the Host Administrator, including the following:

- Accessing the operating system
- Configuring device and application settings
- Managing Host Operators
- Deleting stored tests

Incident response and management

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

Software Bill of Materials

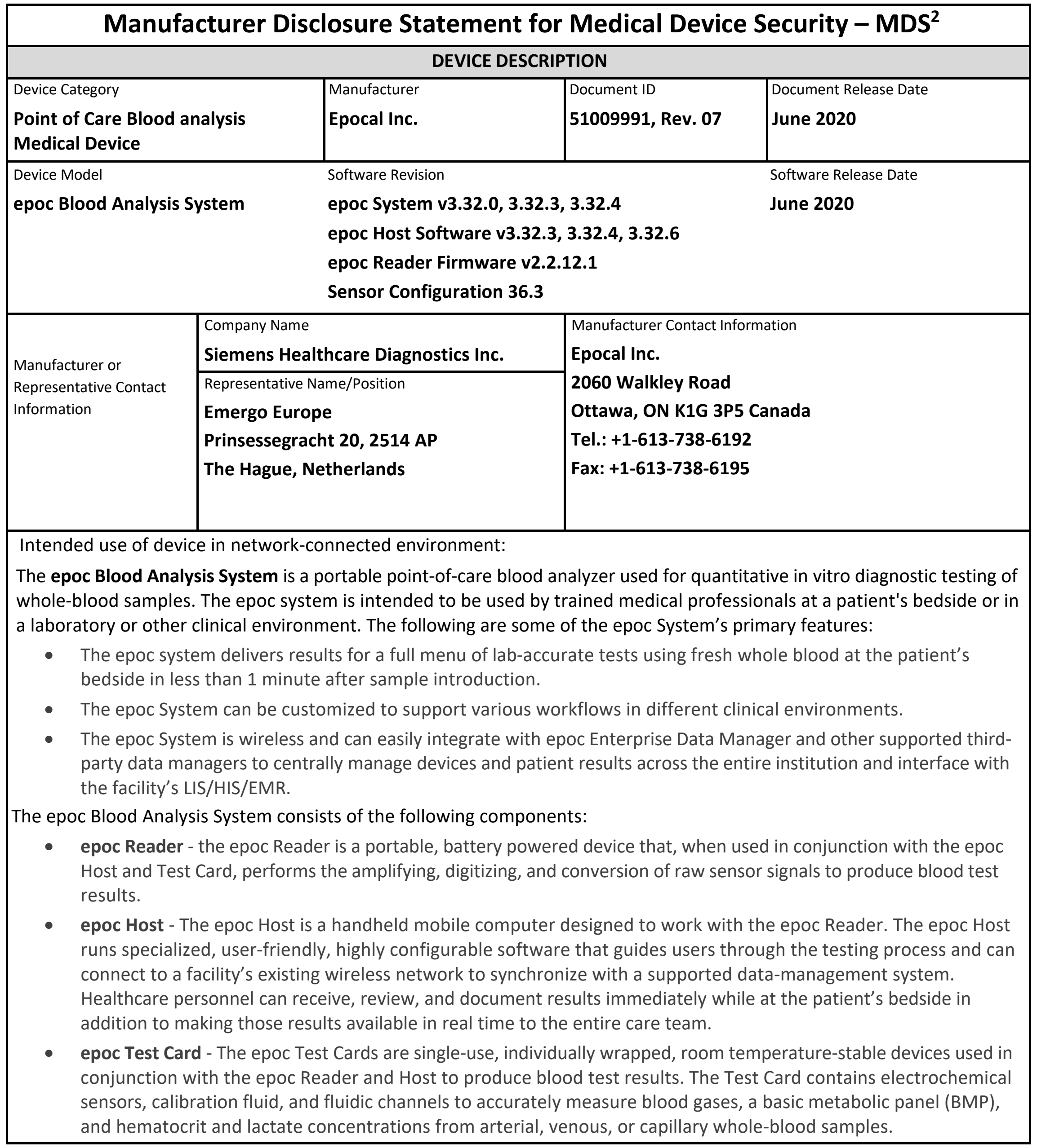
The following table lists the most relevant third-party technologies used.

Vendor Name	Component Name	Component Version	Description/Use
MICROSOFT	WINDOWS Embedded Handheld	6.5	Operating system
ZEBRA	BSP	04.47.0010	OS image for Zebra Model MC55A0
ZEBRA	BSP	02.57.00	OS image for Zebra Model MC55E0
ZEBRA	Wireless Fusion	3.00.2.0.043	WIFI client for Zebra MC55A0
ZEBRA	Wireless Fusion	X_2.03.0.0.024R	WIFI client for Zebra MC55E0
32FEET.NET	InTheHand.Net.Personal	2.3.0530.0	.NET BLUETOOTH library
XCEED	Xceed.Compression.dll Xceed.Compression.Formats.dll Xceed.FIleSystem.dll Xceed.Zip.dll	3.2.6279.0	Zip compression library
SOGO	SogouInput_ppc_1.6.1_sweb.CAB	1.6.1	Chinese keyboard
POCKETKEYS	SIPanelChe.dll, SIPanelGrk.dll SIPanelHun.dll, SIPanelPol.dll SIPanelRom.dll, SIPanelRus.dll SIPanelTur.dll	1.0	Soft keyboards for Czech, Greek, Hungarian, Polish, Romanian, Russian, and Turkish

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	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) for IT networks incorporating medical devices.
2	**Instructions for the responsible organization**
2-1	It is NOT a RESPONSIBILITY AGREEMENT according to IEC 80001-1:2010
3	**Risks and hazardous situations**
3-1	Any modification of the platform, the software, or the interfaces of the Device—unless authorized and approved by Siemens AG Healthcare—voids all warranties, liabilities, assertions, and contracts.
	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.
	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 some IT network or storage, are under the responsibility of the RESPONSIBLE ORGANIZATION.
	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.



Manufacturer Disclosure Statement for Medical Device Security – MDS^2

DEVICE DESCRIPTION

Device Category **Point of Care Blood analysis Medical Device**	Manufacturer **Epocal Inc.**	Document ID **51009991, Rev. 07**	Document Release Date **June 2020**
Device Model **epoc Blood Analysis System**	Software Revision **epoc System v3.32.0, 3.32.3, 3.32.4** **epoc Host Software v3.32.3, 3.32.4, 3.32.6** **epoc Reader Firmware v2.2.12.1** **Sensor Configuration 36.3**		Software Release Date **June 2020**

Manufacturer or Representative Contact Information	Company Name **Siemens Healthcare Diagnostics Inc.**	Manufacturer Contact Information **Epocal Inc.** **2060 Walkley Road** **Ottawa, ON K1G 3P5 Canada** **Tel.: +1-613-738-6192** **Fax: +1-613-738-6195**
	Representative Name/Position **Emergo Europe** **Prinsessegracht 20, 2514 AP** **The Hague, Netherlands**	

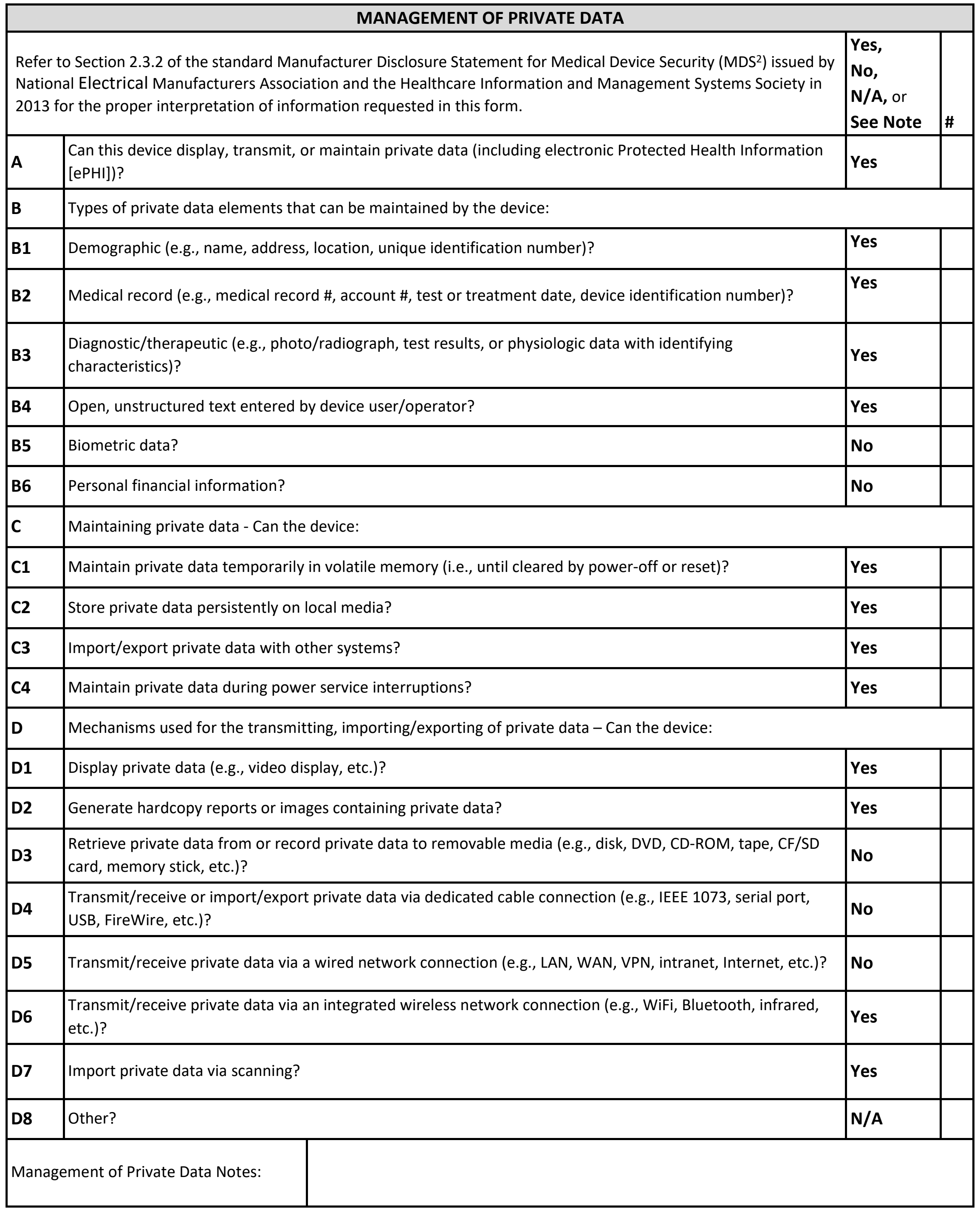
Intended use of device in network-connected environment:

The **epoc Blood Analysis System** is a portable point-of-care blood analyzer used for quantitative in vitro diagnostic testing of whole-blood samples. The epoc system is intended to be used by trained medical professionals at a patient's bedside or in a laboratory or other clinical environment. The following are some of the epoc System's primary features:

- The epoc system delivers results for a full menu of lab-accurate tests using fresh whole blood at the patient's bedside in less than 1 minute after sample introduction.
- The epoc System can be customized to support various workflows in different clinical environments.
- The epoc System is wireless and can easily integrate with epoc Enterprise Data Manager and other supported third-party data managers to centrally manage devices and patient results across the entire institution and interface with the facility's LIS/HIS/EMR.

The epoc Blood Analysis System consists of the following components:

- **epoc Reader** - the epoc Reader is a portable, battery powered device that, when used in conjunction with the epoc Host and Test Card, performs the amplifying, digitizing, and conversion of raw sensor signals to produce blood test results.
- **epoc Host** - The epoc Host is a handheld mobile computer designed to work with the epoc Reader. The epoc Host runs specialized, user-friendly, highly configurable software that guides users through the testing process and can connect to a facility's existing wireless network to synchronize with a supported data-management system. Healthcare personnel can receive, review, and document results immediately while at the patient's bedside in addition to making those results available in real time to the entire care team.
- **epoc Test Card** - The epoc Test Cards are single-use, individually wrapped, room temperature-stable devices used in conjunction with the epoc Reader and Host to produce blood test results. The Test Card contains electrochemical sensors, calibration fluid, and fluidic channels to accurately measure blood gases, a basic metabolic panel (BMP), and hematocrit and lactate concentrations from arterial, venous, or capillary whole-blood samples.



MANAGEMENT OF PRIVATE DATA

	Refer to Section 2.3.2 of the standard Manufacturer Disclosure Statement for Medical Device Security (MDS^2) issued by National Electrical Manufacturers Association and the Healthcare Information and Management Systems Society in 2013 for the proper interpretation of information requested in this form.	**Yes, No, N/A,** or **See 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:		
B1	Demographic (e.g., name, address, location, unique identification number)?	**Yes**	
B2	Medical record (e.g., medical record #, account #, test or treatment date, device identification number)?	**Yes**	
B3	Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)?	**Yes**	
B4	Open, unstructured text entered by device user/operator?	**Yes**	
B5	Biometric data?	**No**	
B6	Personal financial information?	**No**	
C	Maintaining private data - Can the device:		
C1	Maintain private data temporarily in volatile memory (i.e., until cleared by power-off or reset)?	**Yes**	
C2	Store private data persistently on local media?	**Yes**	
C3	Import/export private data with other systems?	**Yes**	
C4	Maintain private data during power service interruptions?	**Yes**	
D	Mechanisms used for the transmitting, importing/exporting of private data – Can the device:		
D1	Display private data (e.g., video display, etc.)?	**Yes**	
D2	Generate hardcopy reports or images containing private data?	**Yes**	
D3	Retrieve private data from or record private data to removable media (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick, etc.)?	**No**	
D4	Transmit/receive or import/export private data via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire, etc.)?	**No**	
D5	Transmit/receive private data via a wired network connection (e.g., LAN, WAN, VPN, intranet, Internet, etc.)?	**No**	
D6	Transmit/receive private data via an integrated wireless network connection (e.g., WiFi, Bluetooth, infrared, etc.)?	**Yes**	
D7	Import private data via scanning?	**Yes**	
D8	Other?	**N/A**	

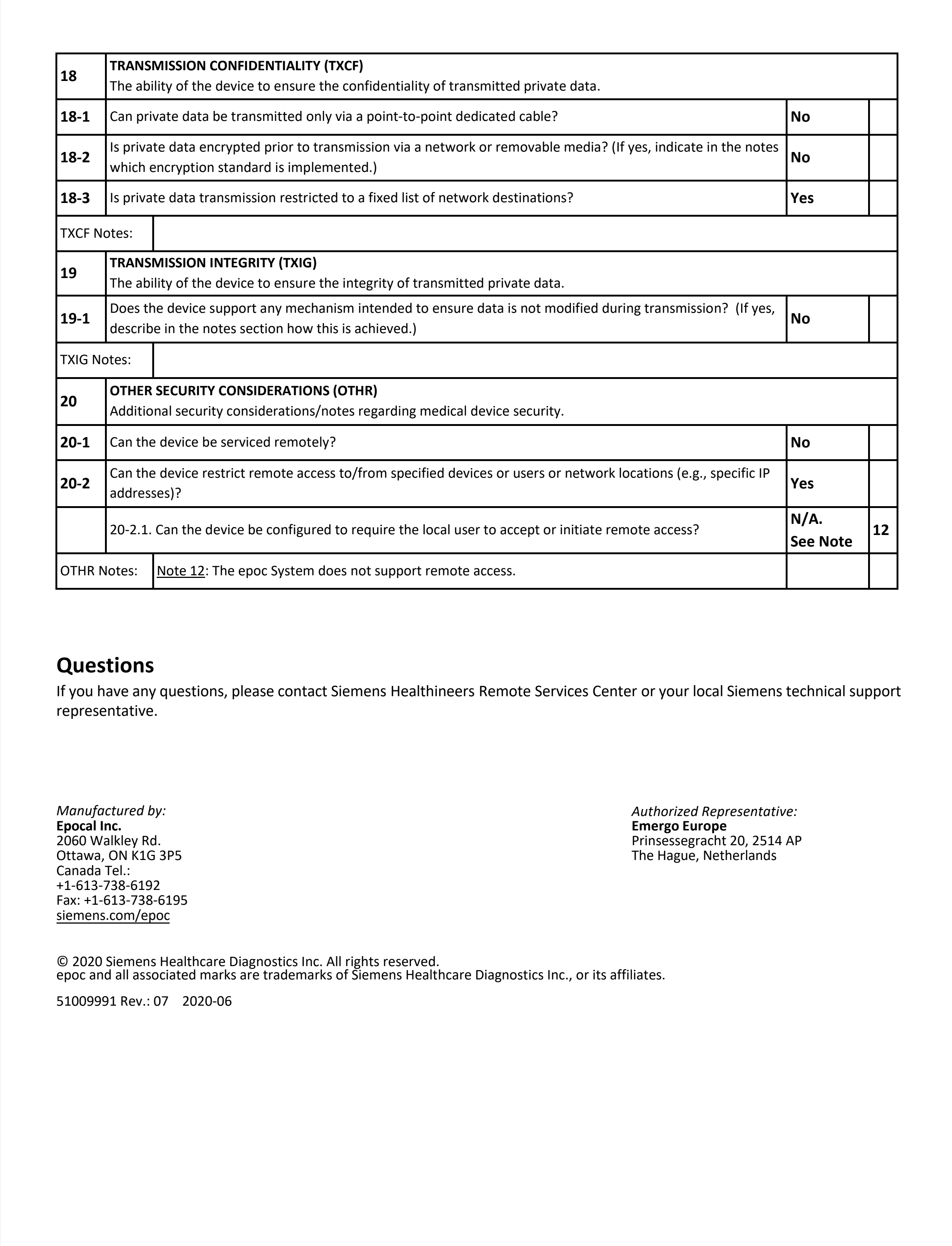
Management of Private Data Notes:

SECURITY CAPABILITIES			
Refer to Section 2.3.2 of the standard Manufacturer Disclosure Statement for Medical Device Security (MDS^2) issued by National Electrical Manufacturers Association and the Healthcare Information and Management Systems Society in 2013 for the proper interpretation of information requested in this form.		**Yes, No, N/A,** or **See 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)?	**Yes**	
	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.)	**Yes, See Note**	**1**
	1-1.2. Can auto-logoff/screen lock be manually invoked (e.g., via a shortcut key or proximity sensor, etc.) by the user?	**Yes**	
ALOF Notes:	Note 1: epoc Host: **Yes** – Inactivity timeout is administrator-configurable (1-5min).		
2	**AUDIT CONTROLS (AUDT)** The ability to reliably audit activity on the device.		
2-1	Can the medical device create an audit trail?	**Yes**	
2-2	Indicate which of the following events are recorded in the audit log:		
	2-2.1. Login/logout	**Yes**	
	2-2.2. Display/presentation of data	**No**	
	2-2.3. Creation/modification/deletion of data	**Yes**	
	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 2-2.5.1. Remote service activity	**Yes. See Note**	**2**
	2-2.6. Other events? (describe in the notes section)	**Yes. See Note**	**3**
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**	
AUDT Notes:	Note 2: When connecting to a compatible data management system. Note 3: Power notifications, barcode scanning, major system events, system errors.		
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?	**Yes**	
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)?	**Yes. See Note**	**4**
AUTH Notes:	Note 4: Only the Host Administrator account can access the operating system and device configuration.		
4	**CONFIGURATION OF SECURITY FEATURES (CNFS)** The ability to configure/reconfigure device security capabilities to meet users' needs.		
4-1	Can the device owner/operator reconfigure product security capabilities?	**No**	
CNFS Notes:			
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?	**Yes**	
	5-1.1. Can security patches or other software be installed remotely?	**Yes. See Note**	**5**
CSUP Notes:	Note 5: Siemens Healthineers releases updates for the epoc Blood Analysis System twice yearly. These updates include application updates and, if available, appropriate operating system updates..		
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?	**Yes. See Note.**	**6**
DIDT notes:	Note 6: The Device provides the ability to delete individual or all test records based on filtering criteria.		
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)?	**No. See Note**	**7**
DTBK Notes	Note 7: The epoc Host cannot back up to removable media but can transmit records to a compatible data management system for backup.		
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?	**No**	
EMRG notes:			
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?	**Yes**	
IGAU notes:			

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)?	**No**	
	10-1.1. Can the user independently reconfigure antimalware settings?	**No**	
	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?	**No**	
10-2	Can the device owner install or update anti-virus software?	**No**	
10-3	Can only manufacturer-authorized persons repair systems when malware has been detected?	**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?	**No**	
NAUT Notes:			
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?	**Yes**	
12-4	Can default passwords be changed at/prior to installation?	**Yes**	
12-5	Are any shared user IDs used in this system?	**Yes**	
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:			
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 be removed without tools)?	**No, See Note**	**8**
PLOK Notes	Note 8: The epoc Host is a mobile device that is not physically secured.		
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**	**9**
14-2	Is a list of other third party applications provided by the manufacturer available?	**Yes**	
RDMP notes:	Note 9: Microsoft Embedded Handheld v6.5 Zebra Wireless Fusion v3.00		
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.	**No**	
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.)?	**Yes**	
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?	**See Note**	**10**
15-7	Are all communication ports which are not required for the intended use of the device closed/disabled?	**See Note**	**10**
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?	**See Note**	**10**
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?	**See Note**	**10**
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:	Note 10: Host Operators are restricted and cannot access the Operating System or other unnecessary resources. Only Host Administrators can access the Operating System and its resources.		
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. See Note**	**11**
SGUD notes:	Note 11: Refer to epoc System Manual.		
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.)	**No**	
18-3	Is private data transmission restricted to a fixed list of network destinations?	**Yes**	
TXCF Notes:			
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.)	**No**	
TXIG Notes:			
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)?	**Yes**	
	20-2.1. Can the device be configured to require the local user to accept or initiate remote access?	**N/A.** **See Note**	**12**
OTHR Notes:	Note 12: The epoc System does not support remote access.		

Questions

If you have any questions, please contact Siemens Healthineers Remote Services Center or your local Siemens technical support representative.

Manufactured by:
Epocal Inc.
2060 Walkley Rd.
Ottawa, ON K1G 3P5
Canada Tel.:
+1-613-738-6192
Fax: +1-613-738-6195
siemens.com/epoc

Authorized Representative:
Emergo Europe
Prinsessegracht 20, 2514 AP
The Hague, Netherlands

51009991 Rev.: 07 2020-06

Abbreviations

AD	Active Directory
AES	Advanced Encryption Standard
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
HIPAA	Health Insurance Portability and Accountability Act
HIMSS	Healthcare Information and Management Systems Society
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
ICS	Integrated Communication Services
IEC	International Electrotechnical Commission
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
SW	Software
TCP	Transmission Control Protocol
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.

Notes

Notes