Security White Paper and MDS² Form

epoc Blood Analysis System with NXS Host v4.6 and Higher

The facts about the security of our products and solutions

siemens-healthineers.com/epocnxs

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 life cycle 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 component 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

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

- epoc Blood Analysis System provides comprehensive critical care results at the patient's side in less than 1 minute after sample introduction.
- epoc system is integrated for patient safety and delivers a streamlined patient testing process that advances care delivery and accelerates clinical decisions while empowering the laboratory and caregivers to optimize their use of time and resources.
- epoc system is wireless and easily integrates with data management solutions to interface with the facility's LIS/HIS/EMR and centrally manage devices across the entire institution.

epoc Blood Analysis System consists of the following components:

- **epoc Reader:** A portable, battery-powered device that, when used in conjunction with epoc NXS Host and Test Card, performs electrical measurements to produce blood test results.
- **epoc NXS Host:** epoc NXS Host is a handheld mobile computer designed to work with epoc Reader. epoc NXS 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:** epoc Test Cards are single-use, individually wrapped, room temperature-stable devices used in conjunction with 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), eDM Lite.
- **epoc Live Update Service (eLUS):** epoc Live Update Service is an optional online service that can be used to update epoc system software and electronic Value Assignment Datasheets (eVADs) directly over the Internet. This update service can be used by facilities that do not already use EDM, eDM Lite, or another supported data manager software.

Operating systems

- epoc NXS Host: ANDROID 11 (Custom Build v026.13.01)
- epoc Reader: no operating system installed

Hardware specifications

epoc NXS Host:

- Manufacturer: Siemens Healthineers
- Model: PD470SH-B
- CPU: MediaTek MT6762 8 Cortex-4 A53 2.0 GHz/4 A53 1.5 GHz
- Dimensions: 160 mm (H) x 76 mm (W) x 22 mm (D)
- Display: 5.0 in. (127 mm) TFT capacitive touch, Corning Gorilla
- Resolution: 1280 x 720
- Memory: 2 GB RAM, 16 GB flash
- WWAN: N/A
- WLAN: 802.11 a/b/g/n/ac/r (2.4 GHz and 5 GHz)
- WPAN: BLUETOOTH v4.2 (BLE HS-compliant)
- NFC: ISO 14443 Type A/B, FeliCa, MIFARE, and ISO 15693 cards (disabled)
- USB: USB 2.0 (Type C) (used for charging battery)
- microSD slot (maximum 128 GB)
- Front camera: 5 megapixel (disabled)
- Rear camera: 13 megapixel autofocus/LED flash
- Integrated 1D/2D bar-code imager (Zebra SE4710)
- Battery: 4000 mAh (rechargeable)
- Sealing: IP67
- Multiple drops to concrete: 1.5 m across the operating temperature range

epoc Reader:

- Manufacturer: Siemens Healthineers
- CPU: Microchip ARM-based SAM7S256 at 55 MHz
- ULTRALIFE lithium ion rechargeable battery
- BLUETOOTH: Class II v2.1 EDR
- BLUETOOTH module: EZURIO BISM2 or BISMS02BI-01

User account information

epoc NXS Host supports two user types: Host Administrator and Host Operators.

- The Host Administrator is authorized to:
  - Configure WI-FI connectivity
  - Configure date/time
  - Manage Host Operators
  - View, print, and delete stored tests
  - Update device software
  - Update device operating system
- 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
  - View and print stored tests
  - Update device software

Patching strategy

- Siemens Healthineers releases application software for epoc Blood Analysis System twice yearly. These include updates for epoc NXS Host application software, epoc Reader firmware, updated sensor configurations, and operating system updates when available. Updates are available on Siemens Healthineers Document Library (https://doclib.siemens-healthineers.com/home) or via epoc Live Update Service (eLUS).
- Siemens Healthineers does not support installing any nonapproved software on this medical device beyond the software updates provided by Siemens Healthineers.

Cryptography usage

epoc NXS Host optional connection to eLUS

- epoc NXS host connects using an encrypted connection over port 443 to the eLUS service.

Data stored on epoc Reader:

- Data stored on epoc Reader does not contain PHI.
- epoc Reader measures and stores raw conductometric, amperometric, and potentiometric parameters from epoc BGEM Test Card.

Data stored on epoc NXS Host:

- epoc NXS Host stores test records that consist of patient and QA test results, patient demographics, operator-entered parameters, operator information, and other related miscellaneous data.
- epoc NXS Host stores sensitive data, including PHI, using AES-256 encryption.

Data transmitted between epoc NXS Host and Reader:

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

Data transmitted between epoc NXS Host and a supported data manager:

- Patient test records can be transmitted from epoc NXS Host to a supported data manager via the facility's existing 802.11a/b/g/n/ac wireless LAN (WLAN).
- WLAN connections are managed by ANDROID device software and support 802.11a/b/g/n/ac/r using 2.4 GHz and 5 GHz radios.
  Note: 5 GHz is not available in all regions.
- epoc NXS Host supports industry-standard personal and enterprise security protocols including WEP, WPA/WPA2 PSK, WPA/WPA2 Enterprise, and 802.1x EAP.
- epoc NXS Host can be configured to communicate with supported data managers using TLS 1.2.

Handling of sensitive data

epoc Reader:

- Data stored on epoc Reader does not contain PHI.
- epoc Reader measures and stores raw sensor waveforms from each epoc BGEM Test Card and transmits the raw waveforms to epoc NXS Host using BLUETOOTH 2.1 EDR.
- To facilitate troubleshooting, epoc Reader stores the last 20 electronic QC results as well as QC and calibration verification results.

epoc NXS Host:

- epoc NXS Host stores up to 499 blood tests, 2000 QA tests, 500 electronic QC tests, and 500 thermal QA tests.
- Data is purged in first-in, first-out (FIFO) order.
- epoc NXS Host can be configured to automatically delete blood test records after 1 day, 1 week, 1 month, 6 months, 1 year, or when the maximum stored records are reached.
- 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 patient ID (e.g., account number, medical record number, 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, temperature, Fi02, respiratory parameters, Allen test, and free-text comments
  - Patient and QA test results
  - Other miscellaneous data, including application logs and raw diagnostics data received from epoc Reader for analysis
- Raw diagnostics files, application logs, and audit 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 diagnostics files.

Data recovery

epoc NXS Host 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 supported external data management systems, such as POCcelerator® Data Management System.

Device settings can be managed locally on each individual device or centrally using a supported external data management system.

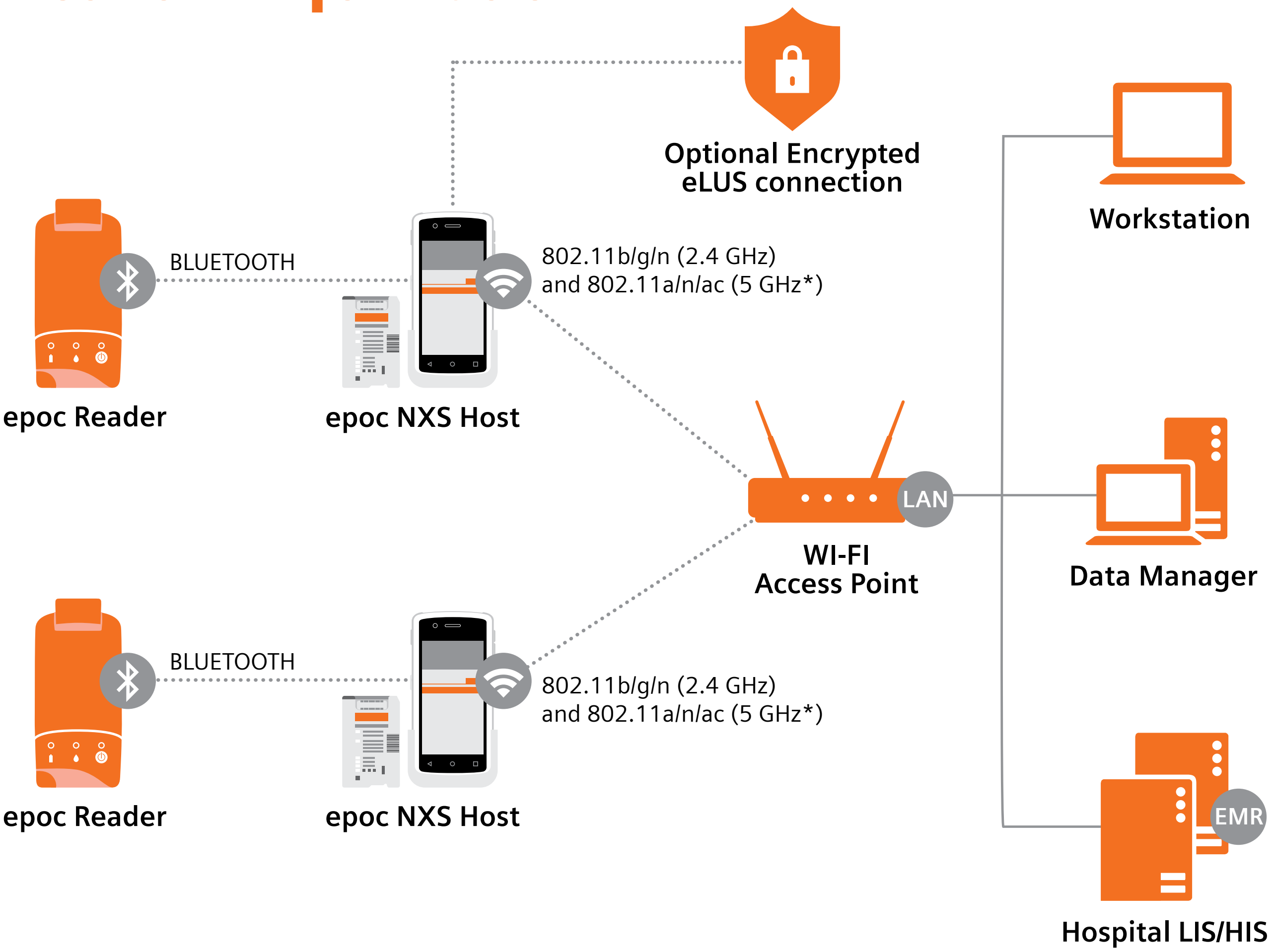
Boundary defense

epoc NXS Host network connectivity is limited to connecting to a data management system via wireless communication. Connections are initiated from epoc NXS Host device. epoc NXS Host does not listen for incoming network connections.

Terms and conditions

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

Network Information



**5 GHz not available in all regions.*

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

Port Number	Service/Function	Direction	Protocol
Configurable	Synchronization with a supported data manager TLS 1.2 end-to-end encryption is supported	Bidirectional	Proprietary
443	Optional, encrypted connection to eLUS	Unidirectional	Proprietary

Allowed Services

Service	Description	Startup Type	Log On As
IMCP echo	Respond to ICMP echo request (ping)	Automatic	NA
DHCP Client	Dynamic Host Configuration Protocol client; automates configuring the device on IP networks.	Automatic	NA
DNS Client	Domain Name Service client; resolve DNS requests using an external DNS server.	Automatic	NA

Security Controls

Malware protection

- epoc NXS Host does not support anti-virus or anti-malware software.
- 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.
- System is configured to prevent access to the underlying operating system.

Authentication authorization controls

- 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:
  - 4–20 characters in length
  - One or more uppercase characters
  - One or more lowercase characters
  - One or more numeric character (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 login attempts.

Continuous vulnerability assessment and remediation

All third-party components are registered with Siemens Vulnerability Monitoring and are reviewed and monitored for vulnerabilities which may affect the product.

Hardening

- epoc system is a closed system configured to prevent access to the underlying operating system.
- Unnecessary ports and services are disabled.
- Auto-launch of executables when removable media is inserted has been disabled.
- epoc NXS Host design allows more control over which applications and system services are included and excluded in the operating system image, which helps minimize the attack surface.

Network controls

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

Physical protection

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

Auditing/logging

- Device application logs track system events and user activities.

Remote connectivity

epoc system does not support remote connections.

Administrative controls

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

- Configuring WI-FI connections
- Configuring epoc 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.

Shared Responsibilities

- Maintain the system in a physically restricted environment to limit access. Only appropriately trained and authorized operators should interact with the system.
- The following security-related epoc NXS Host settings are recommended:
  - Security model = Role-Based
  - Authorization to run tests = ID Only

    Note: Requiring a password to run a test is not recommended.
  - Authorization to view test history = “ID and Password”
  - Automatic logout after inactivity = Enabled
  - Inactivity timer = 15 (minutes) or less
- epoc NXS Host can be configured to manage operators locally on each individual system or centrally using an informatics data management system. When operators are managed via informatics, the data manager will send a complete operator list that replaces all existing operators.
- When connecting the system 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 (nor desired).
- Update the software when new versions are provided by Siemens Healthineers.
- Informatics data management systems should be deployed on secure servers that prevent unauthorized access.

Software Bill of Materials

The following table lists the most relevant third-party technologies used (updated 16 November 2023).

Vendor Name	Component Name	Component Version	Description/Use
GOOGLE	Base OS	11	ANDROID OS
ARBOR SOLUTION Inc.	Custom ANDROID OS	026.13.01	Operating system – custom build
ARBOR SOLUTION Inc.	pd470-apis	v1.7	Custom OS platform SDK header
REALM	REALM JAVA	10.13.0	No-SQL database
GOOGLE, Inc.	Protobuf-life Protobuf Gradle plugin	3.0.0 0.8.3	Cross-platform RPC framework
GOOGLE, Inc.	Dagger	2.36	Dependency Injection framework
GITHUB project, multiple contributors	RXJava library	3.1.5	Reactive programming framework for JAVA
GITHUB project, multiple contributors	RXANDROID	3.0.2	Reactive programming framework for ANDROID
GITHUB project, Srikanth Lingala	zip4j	2.11.2	File compression/encryption library
GREENROBOT Org.	Eventbus	3.0.0	Asynchronous messaging framework
AIDAN FOLESTAD	MaterialDialog	0.9.4.7	UI control
KASUAL	MaterialNumberPicker	1.2.1	UI control
SQUARE Inc.	retrofit2	2.4.0	REST client (HTTP)

Manufacturer Disclosure Statement according to IEC 60601-1

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 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) 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 to some 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.
	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.

Manufacturer Disclosure Statement for Medical Device Security—MDS^2

Question ID	Question	Answer	Notes
DOC-1	Manufacturer Name	Siemens Healthineers	–
DOC-2	Device Description	epoc® Blood Analysis System with epoc NXS Host is a portable point-of-care blood analyzer used for quantitative in vitro diagnostic testing of whole blood samples. epoc NXS 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 epoc NXS system's primary features: epoc system with epoc NXS Host delivers results for a full menu of lab-accurate tests using fresh whole blood at the patient's bedside in less than one minute after sample introduction. These tests include pH, pCO^2, pO^2, Na$^+$, K$^+$, Ca^{++}, Cl$^-$, TCO^2, Glucose, Lactate, BUN (Urea), Creatinine, Hct, and associated calculated parameters. epoc system can be customized to support various workflows in different clinical environments. epoc system is wireless and can easily integrate with POCcelerator® Data Management System and other supported data managers to centrally manage devices and patient results across the entire institution and interface with the facility's LIS/HIS/EMR.	–
DOC-3	Device Model	epoc Blood Analysis System with epoc NXS Host	–
DOC-4	Document ID	51017277, Rev. 03	–
DOC-5	Manufacturer Contact Information	https://www.siemens-healthineers.com/how-can-we-help-you	–
DOC-6	Intended use of device in network-connected environment	Transmit patient, quality assurance, electronic QC results to supported data management systems and laboratory information system (LIS). Receive certified operators, device settings, software updates.	–
DOC-7	Document Release Date	April 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 of Product and Solution Security White Paper for the product.	–
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	–

Management of Personally Identifiable Information

Question ID	Question	Answer	Notes
MPII-1	Can this device display, transmit, store, or modify personally identifiable information (e.g. electronic Protected Health Information (ePHI))?	Yes	epoc NXS Host stores test records that consist of patient and QA test results, patient demographics, operator-entered parameters, operator information, respiratory parameters, critical result notification information, and other related miscellaneous data. Test records may consist of the following data: • Patient demographics, including patient ID (e.g., account number, medical record number, 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, temperature, Fi02, respiratory parameters, Allen test, and free-text comments • Patient and QA test results • Other miscellaneous data, including application logs and raw diagnostics data received from the epoc Reader for analysis
MPII-2	Does the device maintain personally identifiable information?	Yes	–
MPII-2.1	Does the device maintain personally identifiable information temporarily in volatile memory (i.e., until cleared by power-off or reset)?	Yes	–
MPII-2.2	Does the device store personally identifiable information persistently on internal media?	Yes	–
MPII-2.3	Is personally identifiable information preserved in the device's non-volatile memory until explicitly erased?	Yes	Each epoc system maintains up to 499 patient records. Records are automatically deleted in a first-in/first-out order.
MPII-2.4	Does the device store personally identifiable information in a database?	Yes	epoc system stores patient results in a Realm No-SQL database accessible only on the device.
MPII-2.5	Does the device allow configuration to automatically delete local personally identifiable information after it is stored to a long term solution?	Yes	Device can be configured to delete patient tests after a period of time.
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	epoc system has the option to communicate with a supported point-of-care data management system such as POCcelerator system to transmit patient samples and optionally obtain patient demographics from the remote system based on patient ID.
MPII-2.7	Does the device maintain personally identifiable information when powered off, or during power service interruptions?	Yes	–
MPII-2.8	Does the device allow the internal media to be removed by a service technician (e.g., for separate destruction or customer retention)?	No	–
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	–

Question ID	Question	Answer	Notes
MPII-3	Does the device have mechanisms used for the transmitting, importing/exporting of personally identifiable information?	Yes	Optional
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	Optional mobile printer
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.)?	No	epoc system is a portable handheld containing built-in flash memory where PII is stored.
MPII-3.4	Does the device transmit/receive or import/export personally identifiable information via dedicated cable connection (e.g., RS-232, RS-423, USB, FireWire, etc.)?	No	–
MPII-3.5	Does the device transmit/receive personally identifiable information via a wired network connection (e.g., RJ45, fiber optic, etc.)?	No	–

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	Answer	Notes
ALOF-1	Can the device be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., auto log off, session lock, password protected screen saver)?	Yes	By default, epoc NXS Host will log off the user after 5 minutes of inactivity. This setting is configurable to 1, 5, 15, 30, 45, 60 minutes.
ALOF-2	Is the length of inactivity time before auto log off/ screen lock user or administrator configurable?	Yes	Administrator only

Audit Controls (AUDT)

The ability to reliably audit activity on the device.

Question ID	Question	Answer	Notes
AUDT-1	Can the medical device create additional audit logs or reports beyond standard operating system logs?	Yes	–
AUDT-1.1	Does the audit log record a USER ID?	Yes	–
AUDT-1.2	Does other personally identifiable information exist in the audit trail?	–	–
AUDT-2	Are events recorded in an audit log? If yes, indicate which of the following events are recorded in the audit log:	Yes	–
AUDT-2.1	Successful login/logout attempts?	Yes	–
AUDT-2.2	Unsuccessful login/logout attempts?	Yes	–
AUDT-2.3	Modification of user privileges?	Yes	–
AUDT-2.4	Creation/modification/deletion of users?	Yes	–
AUDT-2.5	Presentation of clinical or PII data (e.g. display, print)?	Yes	–
AUDT-2.6	Creation/modification/deletion of data?	Yes	–
AUDT-2.7	Import/export of data from removable media (e.g. USB drive, external hard drive, DVD)?	No	–
AUDT-2.8	Receipt/transmission of data or commands over a network or point-to-point connection?	Yes	–
AUDT-2.8.1	Remote or on-site support?	No	–
AUDT-2.8.2	Application Programming Interface (API) and similar activity?	No	–
AUDT-2.9	Emergency access?	Yes	–

Question ID	Question	Answer	Notes
AUDT-2.10	Other events (e.g., software updates)?	Yes	–
AUDT-2.11	Is the audit capability documented in more detail?	Yes	–
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?	Yes	–
AUDT-4.1	Does the audit log record date/time?	Yes	–
AUDT-4.1.1	Can date and time be synchronized by Network Time Protocol (NTP) or equivalent time source?	Yes	–
AUDT-5	Can audit log content be exported?	Yes	–
AUDT-5.1	Via physical media?	No	–
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	–
AUDT-5.4	Are audit logs encrypted in transit or on storage media?	Yes	–
AUDT-6	Can audit logs be monitored/reviewed by owner/operator?	No	–
AUDT-7	Are audit logs protected from modification?	Yes	–
AUDT-7.1	Are audit logs protected from access?	Yes	–
AUDT-8	Can audit logs be analyzed by the device?	No	–

Authorization (AUTH)

The ability of the device to determine the authorization of users.

Question ID	Question	Answer	Notes
AUTH-1	Does the device prevent access to unauthorized users through user login requirements or other mechanism?	Yes	An operator ID and password is required for access.
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?	No	–
AUTH-2	Can users be assigned different privilege levels based on "role" (e.g., user, administrator, and/or service, etc.)?	Yes	epoc NXS Host supports two user types with different permissions: one Host Administrator and multiple Host Operators who perform blood testing.
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	epoc NXS Host prevents the user from exiting the application UI. This prevents access to functionality outside of what is presented by epoc NXS Host user interface.

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.

Question ID	Question	Answer	Notes
CSUP-1	Does the device contain any software or firmware which may require security updates during its operational life, either from the device manufacturer or from a third-party manufacturer of the software/firmware? If no, answer "N/A" to questions in this section.	Yes	–
CSUP-2	Does the device contain an Operating System? If yes, complete 2.1–2.4.	Yes	–
CSUP-2.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	Yes	Refer to the epoc System with epoc NXS Host Manual.
CSUP-2.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	No	–
CSUP-2.3	Does the device have the capability to receive remote installation of patches or software updates?	Yes	Optionally retrieve software, OS update, and Electronic Value Assignment Datasheet (eVAD) using epoc Live Update Service (eLUS).
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	Refer to the epoc System with epoc NXS Host Manual.
CSUP-3.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	No	–
CSUP-3.3	Does the device have the capability to receive remote installation of patches or software updates?	Yes	Optionally retrieve software, OS update, and Electronic Value Assignment Datasheet (eVAD) using epoc Live Update Service (eLUS).
CSUP-3.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	No	–
CSUP-4	Does the device contain Anti-Malware Software? If yes, complete 4.1–4.4.	No	–
CSUP-4.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	N/A	–
CSUP-4.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	N/A	–
CSUP-4.3	Does the device have the capability to receive remote installation of patches or software updates?	N/A	–
CSUP-4.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	N/A	–
CSUP-5	Does the device contain Non-Operating System commercial off-the-shelf components? If yes, complete 5.1–5.4.	Yes	–
CSUP-5.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	Yes	Refer to the epoc System with epoc NXS Host Manual.

Question ID	Question	Answer	Notes
CSUP-5.2	Does the device require vendor or vendor-authorized 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?	Yes	Optionally retrieve software, OS update, and Electronic Value Assignment Datasheet (eVAD) using epoc Live Update Service (eLUS).
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 reference in notes and complete 6.1–6.4.	No	–
CSUP-6.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	N/A	–
CSUP-6.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	N/A	–
CSUP-6.3	Does the device have the capability to receive remote installation of patches or software updates?	N/A	–
CSUP-6.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	N/A	–
CSUP-7	Does the manufacturer notify the customer when updates are approved for installation?	Yes	Release notes are published in Siemens Healthineers Document Library. https://doclib.siemens-healthineers.com/documents
CSUP-8	Does the device perform automatic installation of software updates?	See Notes	No unless integrating with supported data management software such as POCcelerator Data Management System from Siemens Healthineers.
CSUP-9	Does the manufacturer have an approved list of third-party software that can be installed on the device?	No	The user is prevented from installing any third-party software on epoc NXS Host.
CSUP-10	Can the owner/operator install manufacturer-approved third-party software on the device themselves?	No	–
CSUP-10.1	Does the system have mechanism in place to prevent installation of unapproved software?	Yes	Users are prevented from installing any software other than approved epoc NXS Host Software updates.
CSUP-11	Does the manufacturer have a process in place to assess device vulnerabilities and updates?	Yes	Device vulnerabilities and updates are assessed with static code analysis scans and security vulnerability monitoring.
CSUP-11.1	Does the manufacturer provide customers with review and approval status of updates?	Yes	Release notes for available versions of software are provided in the Siemens Healthineers Document Library. See https://doclib.siemens-healthineers.com/documents.
CSUP-11.2	Is there an update review cycle for the device?	Yes	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.

Health Data De-Identification (DIDT)

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

Question ID	Question	Answer	Notes
DIDT-1	Does the device provide an integral capability to deidentify personally identifiable information?	No	–
DIDT-1.1	Does the device support de-identification profiles that comply with the DICOM standard for deidentification?	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.

Question ID	Question	Answer	Notes
DTBK-1	Does the device maintain long term primary storage of personally identifiable information/patient information (e.g. PACS)?	No	–
DTBK-2	Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer?	No	–
DTBK-3	Does the device have an integral data backup capability to removable media?	No	–
DTBK-4	Does the device have an integral data backup capability to remote storage?	Yes	Patient and QC test results can be transmitted an informatics data management system. epoc system does not provide the capability to restore/import patient and QC test results from external storage.
DTBK-5	Does the device have a backup capability for system configuration information, patch restoration, and software restoration?	See Notes	epoc system can integrate with a supported informatics data management system to centrally manage devices and patient results and interface with the facility's LIS/HIS/EMR.
DTBK-6	Does the device provide the capability to check the integrity and authenticity of a backup?	No	If epoc system application becomes corrupted and no longer functions, the device must be returned to Siemens Healthineers Service.

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 nonauthorized manner and is from the originator.

Question ID	Question	Answer	Notes
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).

Question ID	Question	Answer	Notes
MLDP-1	Is the device capable of hosting executable software?	Yes	–
MLDP-2	Does the device support the use of anti-malware software (or other anti-malware mechanism)? Provide details or reference in notes.	No	–
MLDP-2.1	Does the device include anti-malware software by default?	No	–
MLDP-2.2	Does the device have anti-malware software available as an option?	No	–
MLDP-2.3	Does the device documentation allow the owner/operator to install or update anti-malware software?	No	–
MLDP-2.4	Can the device owner/operator independently (re-)configure anti-malware settings?	N/A	–
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?	N/A	–
MLDP-2.7	Are malware notifications written to a log?	No	–
MLDP-2.8	Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)?	N/A	epoc NXS Host does not support anti-virus or anti-malware software.
MLDP-3	If the answer to MLDP-2 is NO, and anti-malware cannot be installed on the device, are other compensating controls in place or available?	Yes	Refer to the epoc Blood Analysis System with NXS Host Security White Paper for more details. epoc system is a closed system configured to prevent access to the underlying operating system. Unnecessary ports and services are disabled. Auto-launch of executables when removable media is inserted has been disabled. epoc NXS Host design allows more control over which applications and system services are included and excluded in the operating system image, which helps minimize the attack surface. epoc NXS Host network connectivity is limited to connecting to a data management system via wireless communication. Connections are initiated from epoc NXS Host device. epoc NXS Host does not listen for incoming network connections.
MLDP-4	Does the device employ application whitelisting that restricts the software and services that are permitted to be run on the device?	No	–
MLDP-5	Does the device employ a host-based intrusion detection/prevention system?	No	–
MLDP-5.1	Can the host-based intrusion detection/prevention system be configured by the customer?	N/A	–
MLDP-5.2	Can a host-based intrusion detection/prevention system be installed by the customer?	N/A	–

Node Authentication (NAUT)

The ability of the device to authenticate communication partners/nodes.

Question ID	Question	Answer	Notes
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)?	See Notes	TLS connections to a data manager using trusted certificates are supported.
NAUT-2	Are network access control mechanisms supported (E.g., does the device have an internal firewall, or use a network connection white list)?	No	epoc NXS System application does not listen for any external connection requests. If using a supported data manager, there is a single, device-initiated TCP connection to the data manager. Device does not use domain resources. There is no internal firewall.
NAUT-2.1	Is the firewall ruleset documented and available for review?	N/A	–
NAUT-3	Does the device use certificate-based network connection authentication?	Yes	TLS connections to a data manager using trusted certificates are supported.

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.

Question ID	Question	Answer	Notes
CONN-1	Does the device have hardware connectivity capabilities?	Yes	epoc system with epoc NXS Host supports connections to WI-FI 802.11 network access and BLUETOOTH 2.1 EDR. WI-FI is not required to operate the instrument. BLUETOOTH is required for the instrument to operate.
CONN-1.1	Does the device support wireless connections?	Yes	–
CONN-1.1.1	Does the device support Wi-Fi?	Yes	WLAN connections are managed by ANDROID device software and support 802.11a/b/g/n/ac/r using 2.4 GHz and 5 GHz radios. epoc NXS Host supports industry-standard personal and enterprise security protocols including WPA/WPA2 PSK, WPA/WPA2 Enterprise, and 802.1x EAP.
CONN-1.1.2	Does the device support Bluetooth?	Yes	Data is transmitted between epoc Reader and epoc NXS Host using BLUETOOTH 2.1 EDR and is encrypted using BLUETOOTH standard 128-bit encryption with PIN authentication. BLUETOOTH Low Energy (BLE) is not supported.
CONN-1.1.3	Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)?	No	–
CONN-1.1.4	Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)?	No	–
CONN-1.2	Does the device support physical connections?	No	–
CONN-1.2.1	Does the device have available RJ45 Ethernet ports?	No	–
CONN-1.2.2	Does the device have available USB ports?	Yes	epoc NXS Host has a USB port. epoc NXS Host prevents external devices (e.g., laptops) from communicating with it by disabling the ANDROID device bridge (ADB). epoc Reader has a USB port that is disabled at the factory.
CONN-1.2.3	Does the device require, use, or support removable memory devices?	See Notes	epoc NXS Host supports use of a microSD card for the purpose of epoc software updates.
CONN-1.2.4	Does the device support other physical connectivity?	No	–

Question ID	Question	Answer	Notes
CONN-2	Does the manufacturer provide a list of network ports and protocols that are used or may be used on the device?	Yes	epoc NXS Host can be a client to supported data manager server applications to communicate using a proprietary protocol. epoc NXS Host application does not have any open external listening ports.
CONN-3	Can the device communicate with other systems within the customer environment?	Yes	epoc NXS Host can communicate with a supported data manager.
CONN-4	Can the device communicate with other systems external to the customer environment (e.g., a service host)?	Yes	If device is connected to internet, option is available to receive software update online from epoc Live Update Service (eLUS).
CONN-5	Does the device make or receive API calls?	No	epoc System does not provide an API for external access and does not interact with any external system APIs. Data transmitted between epoc Reader and epoc NXS Host includes raw measurement and QA data and does not contain PHI. Optional communication with data manager servers is done over LAN/WLAN using a proprietary protocol.
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	TLS v1.2 connection to a data manager is supported. epoc NXS Host does not send any outbound authentication certificates.
CONN-7.1	Is TLS configurable?	Yes	Use of TLS is optional for data manager connections. Specific TLS parameters are not configurable.
CONN-8	Does the device provide operator control functionality from a separate device (e.g., telemedicine)?	No	–

Person Authentication (PAUT)

The ability to configure the device to authenticate users.

Question ID	Question	Answer	Notes
PAUT-1	Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)?	Yes	–
PAUT-1.1	Does the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)?	See Notes	Host Administrator account authentication is enforced. Host Operator account authentication can be configured to require ID only or ID and password to run and view tests.
PAUT-2	Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, etc.)?	See Notes	epoc NXS Host can be configured to manage operators locally on each individual system or centrally using an informatics data management system. When operators are managed via informatics, the data manager will send a complete operator list that replaces all existing operators.
PAUT-3	Is the device configurable to lock out a user after a certain number of unsuccessful logon attempts?	Yes	Users are locked out after five consecutive failed login attempts. Locked-out accounts can be restored by the Host Administrator account.
PAUT-4	Are all default accounts (e.g., technician service accounts, administrator accounts) listed in the documentation?	Yes	The Host Administrator account is the only default account.
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	–
PAUT-8	Does the device support multi-factor authentication?	No	–

Question ID	Question	Answer	Notes
PAUT-9	Does the device support single sign-on (SSO)?	No	–
PAUT-10	Can user accounts be disabled/locked on the device?	Yes	User accounts are locked after five consecutive failed login attempts. User accounts can be removed by the Host Administrator. If using Informatics operator management, account activation and expiration dates can be configured in the operator list sent by the data manager.
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	Operator IDs and passwords are stored locally on each epoc NXS Host in application-specific AES-256 encrypted storage.
PAUT-14.1	Are credentials stored using a secure method?	Yes	Operator credentials are stored in an AES-256 encrypted database, with the passwords stored as hashed value.

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.

Question ID	Question	Answer	Notes
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)?	No	epoc System is a portable patient-side testing device. PHI/PII is stored in a database in memory that is physically embedded on epoc NXS Host.
PLOK-3	Are all device components maintaining personally identifiable information (other than removable media) physically secured behind an individually keyed locking device?	No	epoc NXS System is a portable patient-side testing device. PHI/PII is stored in a database in memory that is physically embedded on epoc NXS Host.
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 Components In Device Life Cycle (RDMP)

Manufacturer's plans for security support of third-party components within the device's life cycle.

Question ID	Question	Answer	Notes
RDMP-1	Was a secure software development process, such as ISO/IEC 27034 or IEC 62304, followed during product development?	No	–
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	Software release notes are published in the Siemens Healthineers Document Library. See https://doclib.siemens-healthineers.com/documents
RDMP-4	Does the manufacturer have a plan for managing third-party component end-of-life?	Yes	Third-party software shall be registered with the Siemens ProductCERT Security Vulnerability Monitoring (SVM) service. Where possible, source code of third-party components will be maintained to mitigate risk of the original developer terminating support.

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.

Question ID	Question	Answer	Notes
SBOM-1	Is the SBoM for this product available?	Yes	See the "Software Bill of Materials" section of the epoc NXS System Security White Paper.
SBOM-2	Does the SBoM follow a standard or common method in describing software components?	Yes	See the "Software Bill of Materials" section of the epoc NXS System Security White Paper.
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	"Software Bill of Materials" section of the epoc NXS System Security White Paper includes a short description/ use for each item.
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	Whenever a new version of epoc NXS System software is released, the epoc NXS System Security White Paper is updated and re-released.

System And Application Hardening (SAHD)

The device's inherent resistance to cyber attacks and malware.

Question ID	Question	Answer	Notes
SAHD-1	Is the device hardened in accordance with any industry standards?	No	–
SAHD-2	Has the device received any cybersecurity certifications?	No	–
SAHD-3	Does the device employ any mechanisms for software integrity checking	Yes	epoc system employs digitally signed binaries.
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?	Yes	CRC is used on combined software and operating system upgrade file.
SAHD-3.2	Does the device employ any mechanism (e.g., releases-specific hash key, checksums, digital signature, etc.) to ensure the software updates are the manufacturer-authorized updates?	Yes	Digital signature is used to generate authorized software upgrades.
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	epoc NXS Host supports two user types: Host Administrator and Host Operators. The Host Administrator is authorized to configure epoc settings, configure WI-FI connectivity, set date/time, manage Host Operators, view, print, and delete stored test records, and update device software. Host Operators can be managed directly on the device or on a supported data manager. Host Operators can be authorized to run patient blood tests, run QA tests, view and print stored tests, and update device software.

Question ID	Question	Answer	Notes
SAHD-5.1	Does the device provide role-based access controls?	Yes	epoc NXS Host supports two user types: Host Administrator and Host Operators. The Host Administrator is authorized to configure epoc settings, configure WI-FI connectivity, set date/time, manage Host Operators, view, print, and delete stored test records, and update device software. Host Operators can be managed directly on the device or on a supported data manager. Host Operators can be authorized to run patient blood tests, run QA tests, view and print stored tests, and update device software.
SAHD-6	Are any system or user accounts restricted or disabled by the manufacturer at system delivery?	Yes	There is one Host Administrator account. There are no predefined Host Operator accounts.
SAHD-6.1	Are any system or user accounts configurable by the end user after initial configuration?	Yes	Host Operators can change their own passwords. The Host Administrator can create and delete accounts and change permissions of other accounts.
SAHD-6.2	Does this include restricting certain system or user accounts, such as service technicians, to least privileged access?	No	Host Administrator can change the permissions of Host Operator accounts.
SAHD-7	Are all shared resources (e.g., file shares) which are not required for the intended use of the device disabled?	Yes	epoc NXS Host application prevents access to shared resources by automatically launching the application and preventing the user from exiting the application UI and accessing ANDROID settings. epoc NXS Host application restricts use of microSD card for application and OS updates only.
SAHD-8	Are all communication ports and protocols that are not required for the intended use of the device disabled?	Yes	epoc NXS Host debug port (ANDROID device bridge, or adb) is disabled. epoc NXS Host application does not have any open external listening ports. epoc NXS Host application can create a client connection to a data manager. This is initiated and controlled by epoc NXS Host application.
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	Services such as FTP and telnet require third-party app installation or access to the ANDROID device bridge (adb). Third-party app installation and adb are disabled on epoc NXS Host.
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	epoc NXS Host application prevents the operator from launching any other applications.
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	epoc NXS Host boot-loader cannot be configured or overridden to boot from external media.
SAHD-12	Can unauthorized software or hardware be installed on the device without the use of physical tools?	No	–
SAHD-13	Does the product documentation include information on operational network security scanning by users?	No	–
SAHD-14	Can the device be hardened beyond the default provided state?	No	–
SAHD-14.1	Are instructions available from vendor for increased hardening?	N/A	–
SAHD-15	Can the system prevent access to BIOS or other bootloaders during boot?	No	–

Question ID	Question	Answer	Notes
SAHD-16	Have additional hardening methods not included in 2.3.19 been used to harden the device?	Yes	Additional device hardening methods: • epoc NXS Host application is automatically launched and prevents the user from exiting the application UI. • epoc NXS Host debug port is disabled. • epoc NXS Host application disallows installation of other apps. • epoc NXS Host application database is encrypted. • epoc NXS Host application employs role-based access control. • epoc NXS Host application locks out operators after five failed login attempts.

Security Guidance (SGUD)

Availability of security guidance for operator and administrator of the device and manufacturer sales and service.

Question ID	Question	Answer	Notes
SGUD-1	Does the device include security documentation for the owner/operator?	Yes	Refer to the epoc System with epoc NXS Host Manual and the epoc System with NXS Host Security White Paper.
SGUD-2	Does the device have the capability, and provide instructions, for the permanent deletion of data from the device or media?	Yes	Host Administrator has the option of deleting all patient records, QA test records, and Host Operator accounts.
SGUD-3	Are all access accounts documented?	Yes	Refer to the epoc NXS System Manual and the epoc NXS System Security White Paper.
SGUD-3.1	Can the owner/operator manage password control for all accounts?	Yes	Host Administrator can enable or disable user accounts and can change the password of other users. Operator accounts can also be managed by a data manager. The data manager provides login credentials when adding accounts.
SGUD-4	Does the product include documentation on recommended compensating controls for the device?	Yes	Refer to the "Shared Responsibilities" section of the epoc NXS System Security White Paper.

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.

Question ID	Question	Answer	Notes
STCF-1	Can the device encrypt data at rest?	Yes	The epoc NXS Host application database is encrypted using AES-256.
STCF-1.1	Is all data encrypted or otherwise protected?	Yes	All data is protected by storage in an encrypted database.
STCF-1.2	Is the data encryption capability configured by default?	Yes	–
STCF-1.3	Are instructions available to the customer to configure encryption?	No	Encryption is not configurable.
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	The encrypted database is located in epoc NXS Host device storage in embedded memory.
STCF-4	Is the data stored in a database external to the device?	No	–

Transmission Confidentiality (TXCF)

The ability of the device to ensure the confidentiality of transmitted personally identifiable information.

Question ID	Question	Answer	Notes
TXCF-1	Can personally identifiable information be transmitted only via a point-to-point dedicated cable?	No	PHI/PII can be transmitted over wireless ethernet to a data manager.
TXCF-2	Is personally identifiable information encrypted prior to transmission via a network or removable media?	See Notes	epoc NXS Host has a configuration option to encrypt transmissions to/from a data manager using the TLS protocol.
TXCF-2.1	If data is not encrypted by default, can the customer configure encryption options?	Yes	epoc NXS Host has a configuration option to encrypt transmissions to/from a data manager using the TLS protocol.
TXCF-3	Is personally identifiable information transmission restricted to a fixed list of network destinations?	Yes	epoc NXS Host may transmit PHI/PII to and from a data management server. The server connection endpoint is defined by epoc NXS Host client and can only be configured by a privileged operator.
TXCF-4	Are connections limited to authenticated systems?	Yes	Data management server connections are limited to endpoints authenticated only by the Host Administrator.
TXCF-5	Are secure transmission methods supported/implemented (DICOM, HL7, IEEE 11073)?	Yes	Secure transmission to a data manager is supported via TLS.

Transmission Integrity (TXIG)

The ability of the device to ensure the integrity of transmitted data.

Question ID	Question	Answer	Notes
TXIG-1	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission?	No	Data transmitted between epoc NXS Host and epoc Reader uses BLUETOOTH 2.1 EDR and is encrypted using BLUETOOTH standard 128-bit encryption with PIN authentication. Data includes raw measurement and QA data that does not contain PHI/PII. Communication between epoc NXS Host and a data manager uses a proprietary protocol and supports TLS, which provides data integrity.
TXIG-2	Does the device include multiple sub-components connected by external cables?	No	epoc system consists of a display device (epoc NXS Host) connected to one or more epoc Readers via BLUETOOTH. See the "Network Information" section of the epoc System with epoc NXS Host Security White Paper.

Remote Service (RMOT)

Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.

Question ID	Question	Answer	Notes
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?	No	–
RMOT-1.2	Is there an indicator for an enabled and active remote session?	N/A	–
RMOT-1.3	Can patient data be accessed or viewed from the device during the remote session?	N/A	–
RMOT-2	Does the device permit or use remote service connections for predictive maintenance data?	N/A	–
RMOT-3	Does the device have any other remotely accessible functionality (e.g. software updates, remote training)?	Yes	Optional eLUS connection

Other Security Considerations (OTHR)

NONE

Notes:

NONE

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
MDS^2	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 Services
SW	Software
TCP	Transmission Control Protocol
UltraVNC	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, we pioneer breakthroughs in healthcare. For everyone. Everywhere. Sustainably. As a leader in medical technology, we want to advance a world in which breakthroughs in healthcare create new possibilities with a minimal impact on our planet. By consistently bringing innovations to the market, we enable healthcare professionals to innovate personalized care, achieve operational excellence, and transform the system of care.

Our portfolio, spanning in vitro and in vivo diagnostics to image-guided therapy and cancer care, is crucial for clinical decision-making and treatment pathways. With the unique combination of our strengths in patient twinning,* precision therapy, as well as digital, data, and artificial intelligence (AI), we are well positioned to take on the greatest challenges in healthcare. We will continue to build on these strengths to help overcome the world's most threatening diseases, enable efficient operations, and expand access to care.

We are a team of more than 71,000 Healthineers in over 70 countries passionately pushing the boundaries of what is possible in healthcare to help improve the lives of people around the world.

**Personalization of diagnosis, therapy selection and monitoring, aftercare, and managing health.*

Care-Fill, epoc, POCcelerator, and all associated marks are trademarks of Siemens Healthcare Diagnostics Inc., or its affiliates. All other trademarks and brands are the property of their respective owners.

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 Healthineers AG
Siemensstr. 3
91301 Forchheim, Germany
Phone: +49 9191 18-0
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. · POC-23-3005-76 · QR700008901 · 08-2024· ©Siemens Healthcare Diagnostics Inc., 2024