Whitepaper

# Cios Fit VA12 onwards

## Security Whitepaper and MDS²

The facts about the security of our products and solutions

siemens-healthineers.com/cybersecurity

SIEMENS Healthineers

# 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, at the same time, providing measures to strengthen the resiliency of our products from external cybersecurity attackers.

**Vulnerability and incident management**

Siemens Healthineers cooperates with government agencies and cybersecurity researchers concerning reported potential vulnerabilities.

Our communications policy strives for coordinated disclosure.
We work in this way with our customers and other parties, when appropriate, in response to potential vulnerabilities and incidents in our medical devices, no matter what 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
- Security Vulnerability Patches mitigating vulnerabilities in Third Party Software components (including OS) are provided on a regular basis. Please turn to your Service contact for further details.
- 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 of employees to provide knowledge consistent with their level of responsibilities regarding your data and device integrity.

**Contacting Siemens Healthineers about product and solution security**

Siemens Healthineers requests that any cybersecurity or privacy incidents are reported 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

# Contents

# Basic Information

**Cios Fit – Fit for the tough job in the OR.**
Surgery departments are challenged by cost pressure and the need for optimum clinical outcomes. Supposedly cost-effective equipment often compromises quality and reliability and is inadequate in tough surgery environments. To optimally support you, we developed Cios Fit, a multidisciplinary mobile C-arm ready for demanding environments. Based on its built-to-last design, it features powerful state-of-the-art imaging technology and a user-friendly touch-and-play concept.
A system you can rely on – in your demanding OR

**Inventory of devices**
The main operator console of the Cios Fit is in the monitor trolley. It is a **Linux based** SoC with proprietary software. Internally, the software is connected to the x-ray generator, the image intensifier, and the mechanical system via a proprietary Ethernet based protocol.

**Operating systems**
The Cios Fit is a **Linux based system** using the kernel version 3.14.

**Hardware Specifications**
ARM based microprocessor with PCI bus architecture, Linux based system and 128 GB SD card.

**Cryptography usage**
**Cios Fit** utilizes cyphers and protocols built into Linux for encryption and data protection. The following cryptographic algorithms are used:

- AES-256-CBC is used for the encryption of packages.
- SHA512 is used for hashing clinical user information.

**Handling of sensitive data**

- The Cios Fit is designed for temporary data storage. Siemens Healthineers recommends storing this data to a long-term archive, e.g. on a PACS, and subsequently deleting the data on the scanner manually.
- PHI is temporarily stored on the Cios Fit (DICOM raw data)
- PII, as part of the DICOM (PHI) data, is also temporarily stored on the Cios Fit.
- PHI can be transmitted via DICOM.
- PHI can be exported and stored to an external USB drive.
- All Cios Fit product components maintaining sensitive data are physically secure, i.e. cannot be removed without tools. Additionally, secured equipment disassembly at the end of the product lifecycle ensures secured and definite destruction of all sensitive data.

**User account information**
The Cios Fit supports User Management with role-based privilege assignment and access control. User Management is an optional configuration.

**Patching strategy**
Security Vulnerability Patches (SVP) will be provided based on an evaluation of any vulnerabilities and after a validation by Siemens Healthineers to maintain the clinical function of medical device.
SVPs can be installed during a site visit (subject to service contract).

- Technologies and software components are actively monitored for vulnerabilities and availability of security patches.

**Data Recovery**
It is assumed that PHI/PII is archived to a PACS after patient image acquisition is completed or images/reports are ready after post processing.
The system supports backup and restore of system configuration via an external USB drive.

**Boundary Defense**
Built in firewall is used to minimize the network attack surface.
For optimized protection of sensitive data and operation of the system it must be deployed in a secure network environment, utilizing e.g. network segmentation, client access control and protection against access from public networks.
Boundary defenses in the hospital should be multilayered relying on firewalls, proxies, DMZ and network-based IDS and IPS, as well as physical protections.

**Terms and Conditions**
Please also refer to the local Siemens organization for Terms & Conditions related to Cybersecurity.

**Security Skills Assessment and Appropriate Training to Fill Gaps**
The configuration of the system and access control for the CSE is described in the user manual.

# Intended Operational Environment

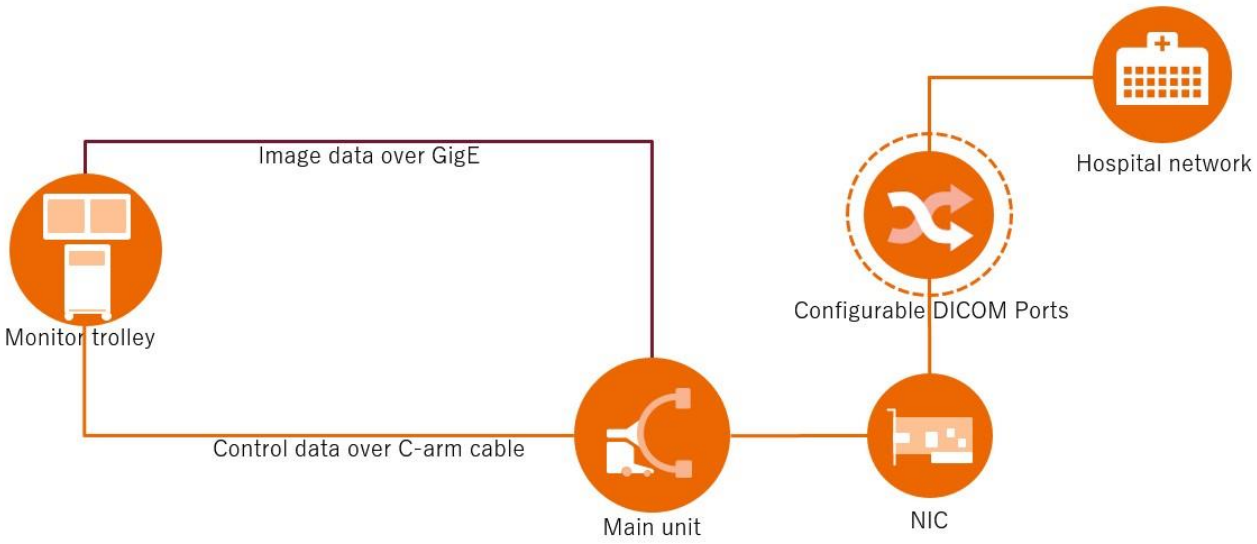


Figure 1 Network Connection for Cios Fit®

| Instructions/Integration | physical access | logical access |
|---|---|---|
| System is placed in a protected zone, no connection to the internet | Clinical users | N/A * |
| System Security is provided and maintained by SHS. | Siemens | N/A * |
| Perimeter security is responsibility of operator. | Clinical users | Clinical users |
| The system provides local protection. | Clinical users | N/A * |
| Default security setup provided by Siemens. | Siemens service | N/A * |
| Incidence handling is provided by Siemens. | Siemens service | N/A * |
| Updates only through Siemens. | Siemens service | N/A * |

* *Note: Siemens Remote Service is not supported.*

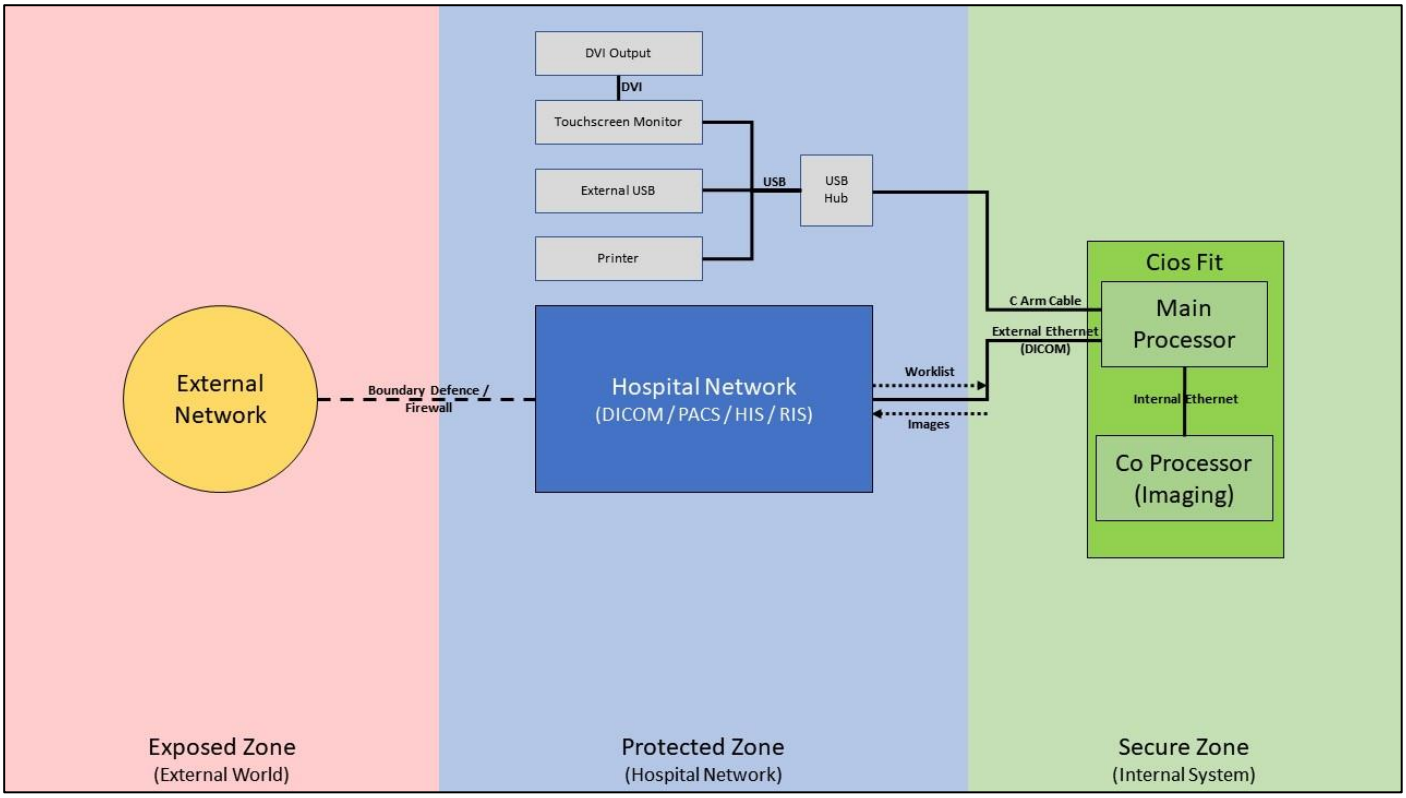


Figure 2 Cios Fit system in an Intended Operational Environment

**Clinical Network Domain**
The network environment is provided and operated by the responsible organization owning and using the Siemens System.
**Clinical Network**
Internal network infrastructure within the hospital is used to exchange images/information via DICOM.
**Siemens System**
The system described here in this Product Security Statement.
**Clinical Firewall**
The component provided by the responsible organization to completely control and restrict the protocol data exchanged between Clinical Network and the Internet.
**DICOM Nodes**
Other systems used for sending images or providing DICOM Images via DICOM protocol or DICOM Worklist to the Siemens System.
**DICOM Printer**
Network Printer to print DICOM Images solely based on DICOM protocol and used with the PRINT functions integrated in the System user interface.
**Printer**
USB Printer, which is accessed by the Siemens system via printer driver and used with the PRINT functions integrated in the System user interface.
**USB Drive**
For exporting images and dose reports in BMP/DICOM formats.

# Security Controls

**Malware protection**
- No malware protection (Linux based product)

**Controlled use of administrative privileges**
- The system distinguishes between clinical and administrative roles. Clinical users don't require administrative privileges. Authorization as a CSE is required for administrative tasks.

**Authentication authorization controls**
- User Name and password based access control for Clinical users when User Management is turned on.
- License based access control for CSE.

**Continuous vulnerability assessment and remediation**
- Vulnerability assessment and remediation is performed.

**Hardening**
- All accounts not required for the intended use of the Cios Fit is disabled or deleted, for both users and applications
- All shared resources (e.g. file shares) not required for the intended use of the Cios Fit is disabled.
- All communication ports not required for the intended use of the Cios Fit is closed/disabled (see Section Network Information)
- All services not required for the intended use for the Cios Fit is deleted/disabled (see Section Network Information)
- All 3rd party software as well as OS-included applications not required for the intended use of the Cios Fit is deleted/disabled (see Section Software Bill of Materials).
- The system control software prohibits boot from removable media.

**Network controls**
- The system is designed to make limited use of network ports and protocols.
- For list of opened ports please refer to Annex X.
- Siemens Healthineers recommends operating the system in a secured network environment, e.g. a separate network segmented or a VPN. In case of a denial of service (DoS) or malware attack, the system can be taken off the clinical network and operated offline. Exchange of clinical result would then require an active offline media (USB drive).
- In-built Linux firewall: Firewall rules are configured so that inbound connections from devices are restricted to minimize the attack surface.

**Physical protection**
- The responsible organization operating the system is responsible for the physical protection of the system and its physical components, e.g. by a technical cabinet room with door locks. Please note that the Cios Fit contains patient data and should be protected against tampering and theft.
- All Cios Fit components maintaining sensitive data (other than removable media) are physically secure, i.e. cannot be removed without tools.

**Data protection controls**
- PHI is protected by role-based access control.
- Auditing of PHI access is possible.

**Auditing/logging**

When User Management is On, the system logs the following events:
- Adding/removing of patients to/from groups.
- Adding/removing of user privileges.
- Adding/editing/deleting user groups.
- Adding/editing/deleting users.
- Audit logs memory full.
- Backup/restore operations successful/unsuccessful.
- BMP/DICOM dose report export successful/unsuccessful and anonymized/non-anonymized.
- BMP/DICOM images export successful/unsuccessful and anonymized/non-anonymized.
- BMP/DICOM SC export successful/unsuccessful and anonymized/non-anonymized.
- BMP/DICOM SR/SCSR export successful/unsuccessful and anonymized/non-anonymized.
- Creating/editing/deleting patients/emergency patient.
- Deleting patient images.
- DICOM ping/echo successful/unsuccessful.
- DICOM worklist operations.
- Export/delete of audit logs.
- Password change successful/unsuccessful.
- System On/Off.
- USB/DICOM print successful/unsuccessful and anonymized/non-anonymized.
- User login/logout successful/unsuccessful.

Additionally, the application software provides the logging for the following:
- System identification (serial number of the system, software version ) and Customer information in the header.
- Event time
- Event code (event ID)
- Event source (source ID of the device which created event)
- Event/Logging description
- Event/logging classification:
  - fatal error
  - error
  - warning
  - information

**Remote connectivity**

The Cios Fit does not support remote connectivity.

**Administrative controls**
- Can assign/de-assign clinical/admin user privileges to/from a user.
- Can share/unshare patients between groups.
- Can create/delete new users/groups.
- Can change passwords for other users/administrators.
- Administrator is also a clinical user.

- Can export/delete Audit logs.

**Incident response and management**

- Incident handling process is defined and executed on demand to deal with cybersecurity incidents.

# Service Log Files

**In case of existing service agreement, logfiles are captured by the CSE to support the following purposes:**

- Improve troubleshooting and system repair by Customer Service.
- Improve system features based on usage information.
- Support customer consulting.

**Log files are used to enable root cause analysis and error correction by Customer Service and Research & Development. PII or PHI is exported and transferred manually, only, when necessary, by the CSE with a prior confirmation from the Customer.**

No Patient Identifiable Information (PII) or Patient Health Information (PHI) is transmitted over logfiles. Only experts involved for the specific error analysis have access to the data (need to know principle) for limited period of time.

The following table describes the service log files created on the Cios Fit with software version VA12 onwards . The list is complete as of today but may change for technical or legal reasons with upcoming software updates and upgrades.

| Logfile | Purpose | PII/PHI | Description/use |
|---|---|---|---|
| <date and time>.tar.gz | Customer Service and Error Analysis | No | System logs, configuration and application traces for error analysis in R&D |
| Installation.log | Customer Service and Error Analysis | No | System software installation logs for error analysis in R&D |
| S34Logs_<date>_<time>.log | Customer Service and Error Analysis | No | Event logs for error analysis in R&D |
| ExposureData.log | Customer Service and Error Analysis | No | X ray exposure information. |

# Shared Responsibility for Security Threats

| Threat | Controls by SHS | Customers Responsibility |
|---|---|---|
| Malware attack to main host computer through hospital network (e.g. virus, ransomware, DoS attacks) | • Execution prevention by default in Linux<br>• Market guidance<br>• System does not provide access to operation system for users | • Operate system in secure subnet<br>  ○ no direct access to the internet<br>  ○ protection of subnet by firewall rules<br>  ○ only necessary ports are routed<br>• Protect network devices adequately against cybersecurity threats<br>• Do not violate intended use<br>• Do not change software/hardware configuration of the system<br>• Implement backup strategy |
| Malware attack to main host computer from local external devices (e.g. USB) | • System does not allow to boot from external media/devices<br>• System does not allow execution of programs from external devices | • Physically protect USB Ports<br>• Scan external media for malware before connecting/inserting to your system |
| Unauthorized access to system | • System provides Service license for access control of the Service user | • Do not share or distribute license files |
| Malware attack to internal system components through wired network connection | • Internal Ethernet port not accessible<br>• Secure protocols are used for communication between the internal system components<br>• Internal network located in monitor cart and C-arm | • Control physical access control to medical system |
| Data disclosure | • All controls mentioned above<br>• SW design: no network access to data base | • All controls mentioned above<br>• Configure only trusted DICOM nodes |
| Data loss, data manipulation | • All controls mentioned above<br>• SW design: no network access to data base | • All controls mentioned above<br>• Configure only trusted DICOM nodes |
| Manipulation of system software | • Encrypted software update or installation packages<br>• Encrypted backup files | • All controls mentioned above |
| Manipulation of acquisition parameters through malware | • All controls mentioned above<br>• Proprietary data protocols are used<br>• Acquisition parameters are only transferred through the internal network<br>• (Data-) Displays show parameters submitted to the acquisition control | • All controls mentioned above<br>• Parameters can be doublechecked with the displayed information |
| Manipulation of service configuration/adjustments | • Service passwords (keys) are generated with state-of-the-art algorithms | • Do not disclose service keys |

# MDS2 with extended information according to IEC60601-1 and IEC80001-1

The MDS2 section contains the mandatory MDS2 form and additional information tables to inform about the

- most relevant third-party technologies used (S-BOM)
- ports provided by the system
- running services
- risk assessment in case of network unavailability

## Manufacturer Disclosure Statement for Medical Device Security – MDS2

### DEVICE DESCRIPTION

| | | | |
|---|---|---|---|
| **(DOC-2) Device Description** Radiographic/Fluoroscopic Units, Mobile | **(DOC-1) Manufacturer Name** see last page | **(DOC-4) Document ID** 11250737-ESK-01S-03 | **(DOC-7) Document Release Date** see last page |
| **(DOC-3) Device Model** Cios Fit | **Software Revision** VA12 onwards | **Software Release Date** 2022-03 | |
| **Manufacturer or Representative Contact Information** | **Company Name** Siemens Healthcare Pvt. Ltd.<br>**Representative Name/Position** For contact information, see last page. | **(DOC-5) Manufacturer Contact Information** see last page | |

**(DOC-6) Intended use of device in network-connected environment:**

Cios Fit is a mobile X-ray system designed to provide X-ray imaging of the anatomical structures of patient during following clinical applications: interventional fluoroscopic, gastro-intestinal, endoscopic, urologic, pain management, orthopedic, neurologic, vascular, cardiac, critical care and emergency room procedures.

Intended purpose of integrating the Device into an IT-Network (see Annex Z for details):
DICOM communication node for image transfer.

| Refer to Section 2.3.2 of NEMA HN 1-2019 standard for the proper interpretation of information requested in this form | Yes, No, N/A, or See Note | Note # |
|---|---|---|
| DOC-8 Coordinated Vulnerability Disclosure: Does the manufacturer have a vulnerability disclosure program for this device? | Yes | |
| DOC-9 ISAO: Is the manufacturer part of an Information Sharing and Analysis Organization? | Yes | 1 |
| DOC-10 Diagram: Is a network or data flow diagram available that indicates connections to other system components or expected external resources? (If yes, provide details or reference in notes) | Yes | 2 |
| DOC-11 SaMD: Is the device Software as a Medical Device (i.e. software-only, no hardware)? (If yes, provide details or reference in notes.) | No | |
| DOC-11.1 Does the SaMD contain an operating system? (See CSUP-2 for more information on device operating system.) | N/A | |
| DOC-11.2 Does the SaMD rely on an owner/operator provided operating system? (If yes, provide details or reference in notes.) | N/A | |
| DOC-11.3 Is the SaMD hosted by the manufacturer? (If yes, provide details or reference in notes.) | N/A | |
| DOC-11.4 Is the SaMD hosted by the customer? (If yes, provide details or reference in notes.) | N/A | |

Device Description (DOC) notes:

1) Siemens Healthineers is part of Health-ISACs
2) See chapter "Intended operational environment" and the P-DPIA for the data flow diagram

## MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATON (MPII)

| Refer to Section 2.3.3 of NEMA HN 1-2019 standard for the proper interpretation of information requested in this form. | Yes, No, N/A, or See Note | Note # |
|---|---|---|
| **MPII** - How personally identifiable information is handled on or by the device. | | |
| MPII-1 Can this **device** display, transmit, store, or modify **personally identifiable information** (e.g. electronic Protected Health Information (ePHI))? (If yes, provide details or reference in notes.) ..... | Yes | 1 |
| 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)? ..... | No | 4 |
| MPII-2.2 Does the **device** store **personally identifiable information** persistently on internal media? ..... | Yes | |
| MPII-2.3 Is **personally identifiable information** preserved in the device's non-volatile memory until explicitly erased? | Yes | |
| MPII-2.4 Does the **device** store **personally identifiable information** in a database? (If yes, provide details or reference in notes.) ..... | Yes | 5 |
| 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 | 6 |
| 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 | 1 |
| MPII-2.7 Does the **device** maintain **personally identifiable information** when powered off, or during power service interruptions? ..... | Yes | 2 |
| MPII-2.8 Does the device allow the internal media to be removed by a service technician (e.g., for separate destruction or customer retention)? ..... | Yes | 3 |
| 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)? | Yes | 5 |
| MPII-3 Does the device have mechanisms used for the transmitting, importing/exporting of personally identifiable information? (Indicate in the notes if the mechanism listed is *optional*.) ..... | Yes | 1 |
| MPII-3.1 Does the **device** display **personally identifiable information** (e.g., video display, etc.)? ..... | Yes | |
| MPII-3.2 Does the **device** generate hardcopy reports or images containing **personally identifiable information**? | Yes | |
| MPII-3.3 Does the **device** retrieve **personally identifiable information** from or record **personally identifiable information** to **removable media** (e.g., removable-HDD, USB memory, DVD-R/RW, CD-R/RW, tape, CF/SD card, memory stick, etc.)? ..... | Yes | |
| MPII-3.4 Does the **device** transmit/receive or import/export **personally identifiable information** via dedicated cable connection (e.g., RS-232, RS-423, USB, FireWire, etc.)? ..... | Yes | 1, 5 |
| MPII-3.5 Does the **device** transmit/receive **personally identifiable information** via a wired network connection (e.g., RJ45, fiber optic, etc.)? ..... | Yes | |
| MPII-3.6 Does the **device** transmit/receive **personally identifiable information** via a wireless network connection (e.g., WiFi, Bluetooth, NFC, infrared, cellular, etc.)? ..... | No | |
| MPII-3.7 Does the **device** transmit/receive **personally identifiable information** over an external network (e.g., Internet)? ..... | No | 7 |
| MPII-3.8 Does the **device** import **personally identifiable information** via scanning a document? ..... | No | |
| MPII-3.9 Does the **device** transmit/receive **personally identifiable information** via a proprietary protocol? ..... | No | |
| MPII-3.10 Does the **device** use any other mechanism to transmit, import or export **personally identifiable information**? (If yes, provide details or reference in notes.) ..... | No | |

Management of personally identifiable information notes:

1. Images are stored on the device in RAW format.
   Images can be exported on a local USB drive in BMP or DICOM format.
   *(optional)* Images can also be exported to a remote DICOM node. For the DICOM Conformance statement see http://siemens.com/dicom or the accompanying documents.
2. Yes, when being connected to mains through UPS.
3. SD card is handed over to the customer for retention or secure erase in case of system refurbishment.
4. LIH is automatically cleared on the closure of a study or a new acquisition.
5. Patient images and database is stored in an internal SD card.
6. Patient data anonymization is possible.
7. DICOM operations are restricted to configured network nodes.

## SECURITY CAPABILITIES

| Refer to Section 2.3.4 and following of NEMA HN 1-2019 standard for the proper interpretation of information requested in this form. | Yes, No, N/A, or See Note | Note # |
|---|---|---|
| **1 AUTOMATIC LOGOFF (ALOF)**<br>The **device**'s ability to prevent access and misuse by unauthorized **users** if **device** is left idle for a period of time. | | |
| ALOF-1 Can the **device** be configured to force reauthorization of logged-in **user**(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)? | No | 1 |
| ALOF-2 Is the length of inactivity time before auto-logoff/screen lock **user** or administrator configurable? (If yes, indicate time, fixed, or configurable range in notes.) | N/A | 1 |
| ALOF notes: 1) The system only supports manual logoff . | | |
| **2 AUDIT CONTROLS (AUDT)**<br>The ability to reliably audit activity on the **device**. | | |
| AUDT-1 Can the **medical device** create additional **audit logs or reports** beyond standard operating system logs? | Yes | |
| AUDT-1.1 Does the audit log record a USER ID? | Yes | |
| AUDT-1.2 Does other personally identifiable information exist in the audit trail? | Yes | 1 |
| 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? | See note | 2 |
| AUDT-2.3 Modification of user privileges? | Yes | 3 |
| AUDT-2.4 Creation/modification/deletion of users? | Yes | |
| AUDT-2.5 Presentation of clinical or PII data (e.g. display, print)? | Yes | 4 |
| AUDT-2.6 Creation/modification/deletion of data? | Yes | 5 |
| AUDT-2.7 Import/export of data from **removable media** (e.g. USB drive, external hard drive, DVD)? | Yes | |
| AUDT-2.8 Receipt/transmission of data or commands over a network or point-to-point connection? | Yes | 6 |
| AUDT-2.8.1 Remote or on-site support? | No | 7 |
| AUDT-2.8.2 Application Programming Interface (API) and similar activity? | No | 7 |
| AUDT-2.9 Emergency access? | Yes | |
| AUDT-2.10 Other events (e.g., software updates)? (If yes, provide details or reference in notes.) | No | |
| AUDT-2-11 Is the audit capability documented in more detail? (If yes, provide details or reference in notes.) | Yes | 8 |
| AUDT-3 Can the owner/operator define or select which events are recorded in the audit log? (If yes, provide details or reference in notes.) | No | |
| AUDT-4 Is a list of data attributes that are captured in the audit log for an event available? (If yes, provide details or reference in notes.) | Yes | 8 |
| 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? | No | |
| AUDT-5 Can audit log content be exported? | Yes | |
| AUDT-5.1 Via physical media? | Yes | 9 |
| AUDT-5.2 Via IHE Audit Trail and Node Authentication (ATNA) profile to SIEM? | No | 9 |
| AUDT-5.3 Via Other communications (e.g., external service device, mobile applications)? (If yes, provide details or reference in notes.) | No | |
| AUDT-5.4 Are audit logs encrypted in transit or on storage media? If yes, provide details or reference in notes. | No | |
| AUDT-6 Can audit logs be monitored/reviewed by owner/operator? (If no, provide details or reference to audit process in notes.) | No | 9, 10 |
| AUDT-7 Are audit logs protected from modification? (If yes, provide details or reference in notes.) | Yes | 9, 10 |
| AUDT-7.1 Are audit logs protected from access? (If yes, provide details or reference in notes.) | Yes | 9, 10 |

| | | | |
|---|---|---|---|
| AUDT-8 Can audit logs be analyzed by the device? (If so, provide reference in notes.)..... | | No | 10 |
| AUDT notes: | 1. User ID, patient details are recorded in the audit log.<br>2. Unsuccessful login attempts are recorded in the audit log.<br>3. Modification of user privileges such as adding/removal of user to groups etc. are recorded in the audit log.<br>4. Printing of PHI is recorded in the audit log.<br>5. Creation/deletion of patients, including emergency patients are recorded in the audit log.<br>6. The system supports only DICOM data exchange over a network.<br>7. SRS is not supported.<br>8. See Security Whitepaper in section “Auditing/logging”.<br>9. Audit logs can only be exported to a local USB drive.<br>10. Viewing audit logs on the system is not supported. | | |

**3 AUTHORIZATION (AUTH)**

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

| | | |
|---|---|---|
| AUTH-1 Does the **device** prevent access to unauthorized **users** through **user** login requirements or other mechanism? | Yes | 1, 2 |
| AUTH-1.1 Can the device be configured to use federated credentials management of users for authorization (e.g., LDAP, OAuth)? (If yes, provide details or reference in notes.) ..... | No | |
| AUTH-1.2 Can the customer push group policies to the device (e.g., Active Directory)? (If yes, provide details or reference in notes.)..... | No | |
| AUTH-1.3 Are any special groups, organizational units, or group policies required? (If yes, provide details or reference in notes.) ..... | No | |
| AUTH-2 Can **users** be assigned different privilege levels based on 'role' (e.g., user, administrator, and/or service, etc.)? | Yes | 3 |
| 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? (If no, provide details or reference in notes.)..... | N/A | 1, 4, 5, 6 |
| AUTH-5 Does the device run in a restricted access mode, or ‘kiosk mode’, by default? (If yes, provide details or reference in notes.) | No | |
| AUTH notes: | 1. User management needs to be turned on. User Management is disabled by default and needs to be turned On by CSE on request of Customer.<br>2. Service user access is access controlled with time-based service licenses<br>3. System administrators and clinical users’ needs to be assigned the respective privileges.<br>4. Secure DICOM, SRS is not supported.<br>5. DICOM operations are restricted to configured network nodes.<br>6. External API requests are not serviced. | |

## SECURITY CAPABILITIES

| Refer to Section 2.3.7 and following of NEMA HN 1-2019 standard for the proper interpretation of information requested in this form. | Yes, No, N/A, or See Note | Note # |
|---|---|---|
| **4 CYBERSECURITY PRODUCT UPGRADES (CSUP)**<br>The ability of on-site service staff, **remote service** staff, or authorized customer staff to install/update **device**'s security patches. | | |
| CSUP-1 Does the device contain any software or firmware which may require security updates during its operational life, either from the device manufacturer or from a third-party manufacturer of the software/firmware? (If no, answer "N/A" to questions in this section.) | Yes | 1 |
| CSUP-2 Does the device contain an Operating System? (If yes, complete CSUP-2.1 to CSUP-2.4.) | Yes | |
| CSUP-2.1 Does the device documentation provide instructions for owner/operator installation of patches or software updates? | No | 1 |
| CSUP-2.2 Does the device require vendor or vendor-authorized service to install patches or software updates? | Yes | 1 |
| CSUP-2.3 Does the device have the capability to receive remote installation of patches or software updates? | No | |
| CSUP-2.4 Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer? | No | |
| CSUP-3 Does the device contain Drivers and Firmware? (If yes, complete CSUP-3.1 to CSUP-3.4.) | Yes | |
| CSUP-3.1 Does the device documentation provide instructions for **owner/operator installation** of patches or software updates? | No | |
| CSUP-3.2 Does the device require **vendor or vendor-authorized** service to install patches or software updates? | Yes | 1 |
| CSUP-3.3 Does the device have the capability to receive **remote installation** of patches or software updates? | No | |
| CSUP-3.4 Does the medical device manufacturer allow security updates from any **third-party manufacturers** (e.g., Microsoft) to be installed without approval from the manufacturer? | No | |
| CSUP-4 Does the device contain Anti-Malware Software? (If yes, complete CSUP-4.1 to CSUP-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 CSUP-5.1 to CSUP-5.4.) | Yes | |
| CSUP-5.1 Does the device documentation provide instructions for **owner/operator installation** of patches or software updates? | No | |
| CSUP-5.2 Does the device require **vendor or vendor-authorized service** to install patches or software updates? | Yes | 1 |
| CSUP-5.3 Does the device have the capability to receive **remote installation** of patches or software updates? | No | |
| CSUP-5.4 Does the medical device manufacturer allow security updates from any **third-party manufacturers** (e.g., Microsoft) to be installed without approval from the manufacturer? | No | |
| CSUP-6 Does the device contain other software components (e.g., asset management software, license management)? (If yes, provide details or reference in notes, and complete CSUP-6.1 to CSUP-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? (If so, provide details or reference in notes.) | Yes | 1, 3 |
| CSUP-8 Does the device perform automatic installation of software updates? | No | |
| CSUP-9 Does the manufacturer have an approved list of third-party software that can be installed on the device? (If so, describe or reference in notes the manufacturer approved third-party software list and/or the manufacturer process for managing requests to approve additional third-party software.) | Yes | 2 |
| 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 | |
| CSUP-11 Does the manufacturer have a process in place to assess device vulnerabilities and updates? | Yes | 1 |

| | | | |
|---|---|---|---|
| CSUP-11-1 | Does the manufacturer provide customers with review and approval status of updates? ..... | No | |
| CSUP-11.2 | Is there an update review cycle for the device? (If so, provide details or reference in notes.) ..... | Yes | 1 |

CSUP notes:

1. Siemens performs vulnerability monitoring of the included third-party components continuously (including operating system). Vulnerabilities are assessed regarding their criticality and safety relevance. In the case of critical vulnerabilities, fixes are distributed.
   Service packs are installed by the CSE.
2. See Annex W
3. Customer information is provided by the CSE.

## SECURITY CAPABILITIES

| Refer to Section 2.3.8 and following of NEMA HN 1-2019 standard for the proper interpretation of information requested in this form. | Yes, No, N/A, or See Note | Note # |
|---|---|---|
| **5 HEALTH DATA DE-IDENTIFICATION (DIDT)**<br>The ability of the **device** to directly remove information that allows identification of a person. | | |
| DIDT-1 Does the device provide an integral capability to de-identify personally identifiable information? (If yes, provide details or reference in notes.) ..... | Yes | 1 |
| DIDT-1.1 Does the device support de-identification profiles that comply with the DICOM standard for de-identification? If so, provide details or reference in notes. ..... | Yes | 1 |
| DIDT notes: 1. As part of DICOM Export or Transfer configuration. Described in DICOM Conformance Statement, available at http://siemens.com/DICOM or see accompanying documents. | | |
| **6 DATA BACKUP AND DISASTER RECOVERY (DTBK)**<br>The ability to recover after damage or destruction of **device** data, hardware, or software. | | |
| 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? | Yes | 1 |
| DTBK-3 Does the **device** have an integral data backup capability to **removable media**? (If yes, provide details or reference in notes.) ..... | Yes | 2, 3 |
| DTBK-4 Does the device have an integral data backup capability to remote storage? (If yes, provide details or reference in notes.) ..... | No | |
| DTBK-5 Does the device have a backup capability for system configuration information, patch restoration, and software restoration? If yes, provide details or reference in notes. ..... | Yes | 3 |
| DTBK-6 Does the device provide the capability to check the integrity and authenticity of a backup? ..... | Yes | |
| DTBK notes: 1. "Factory reset" of the system configuration, imaging and organ programming configurations can be performed using the *Load Default* functionality.<br>2. Backup functionality of device data and SW configuration is provided. Integral data backup capability of ePHI data is provided through the USB and DICOM Interface and export to offline functionality.<br>3. Data (device configuration) backup and restore via an external USB is supported. | | |
| **7 EMERGENCY ACCESS (EMRG)**<br>The ability of the device user to access personally identifiable information in case of a medical emergency situation that requires immediate access to stored personally identifiable information. | | |
| EMRG-1 Does the **device** incorporate an **emergency access** (i.e. "break-glass") feature? (If yes, provide details or reference in notes.) ..... | Yes | 1 |
| EMRG notes: 1. When user management is turned on, the system includes a specific emergency access account. When user management is turned off the system runs with auto-login of a non-privileged user; system is ready for emergency after (re-)start of system. | | |
| **8 HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU)**<br>How the device verifies integrity, verifies authenticity, and assures availability of stored health data on the device. If the device does not store health data, answer "N/A" to questions in this section. | | |
| IGAU-1 Does the **device** provide data integrity checking mechanisms of stored health data (e.g., hash or digital signature)? (If so, provide details or reference in notes.) ..... | No | 1 |
| IGAU-2 Does the device provide error/failure protection and recovery mechanisms for stored health data (e.g., RAID-5)? (If yes, provide details or reference in notes.) ..... | No | 2 |
| IGAU notes: 1. No integrity monitoring is implemented.<br>2. Backup of patient and image data should be done manually to an archive system (PACS) on a regular basis. | | |

## SECURITY CAPABILITIES

| Refer to Section 2.3.12 of NEMA HN 1-2019 standard for the proper interpretation of information requested in this form. | Yes, No, N/A, or See Note | Note # |
|---|---|---|
| **9 MALWARE DETECTION/PROTECTION (MLDP)**<br>The ability of the **device** to effectively prevent, detect and remove malicious software (**malware**). | | |
| MLDP-1 Is the device capable of hosting executable software? | Yes | |
| MLDP-2 Does the **device** support the use of **anti-malware** software (or other **anti-malware** mechanism)? (Provide details or reference in notes.) | No | 1 |
| MLDP-2.1 Does the device include anti-malware software by default? | N/A | |
| MLDP-2.2 Does the device have anti-malware software available as an option? | N/A | |
| MLDP-2.3 Does the **device** documentation allow the owner/operator to install or update anti-malware software? (If yes, provide details or reference in notes.) | N/A | |
| MLDP-2.4 Can the **device** owner/**operator** independently (re-)configure **anti-malware** settings? | N/A | |
| MLDP-2.5 Does notification of malware detection occur in the device user interface? | N/A | |
| MLDP-2.6 Can only manufacturer-authorized persons repair systems when **malware** has been detected? (If yes, provide details or reference in notes.) | N/A | |
| MLDP-2.7 Are malware notifications written to a log? | N/A | |
| MLDP-2.8 Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)? | N/A | |
| MLDP-3 If the answer to MLDP-2 is NO, and anti-malware cannot be installed on the device, are other compensating controls in place or available? If yes, provide details or reference in notes. | N/A | 1 |
| MLDP-4 Does the device employ application whitelisting that restricts the software and services that are permitted to be run on the device? (If yes, provide details or reference in notes.) | Yes | 1, 2 |
| MLDP-5 Does the device employ a host-based intrusion detection/prevention system? (If yes, provide details or reference in notes.) | 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 | |

MLDP notes:
1. Linux based system. Anti-malware software is not required.
2. System software installation packages are encrypted and controlled by Siemens.

| | | |
|---|---|---|
| **10 NODE AUTHENTICATION (NAUT)**<br>The ability of the **device** to authenticate communication partners/nodes. | | |
| NAUT-1 Does the **device** provide/support any means of node authentication that assures both the sender and the recipient of data are known to each other and are authorized to receive transferred information (e.g. Web APIs, SMTP, SNMP)? (If yes, provide details or reference in notes.) | Yes | 1 |
| NAUT-2 Are network access control mechanisms supported (E.g., does the device have an internal firewall, or use a network connection white list)? (If yes, provide details or reference in notes.) | Yes | 2 |
| NAUT-2.1 Is the firewall ruleset documented and available for review? (If yes, provide details or reference in notes.) | Yes | 3 |
| NAUT-3 Does the device use certificate-based network connection authentication? (If yes, provide details or reference in notes.) | No | |

NAUT notes:
1. DICOM operations are restricted to configured network nodes.
2. Inbuilt Linux firewall is used.
3. See Annex X

## SECURITY CAPABILITIES

| Refer to Section 2.3.14 of NEMA HN 1-2019 standard for the proper interpretation of information requested in this form. | Yes, No, N/A, or See Note | Note # |
|---|---|---|
| **11 CONNECTIVITY CAPABILITIES (CONN)**<br>All network and removable media connections must be considered in determining appropriate security controls. This section lists connectivity capabilities that may be present on the device. | | |
| CONN-1 Does the device have hardware connectivity capabilities. If yes, provide details or a reference that identifies the hardware connectivity capabilities of the device. If no, indicate "none" in notes and answer "N/A" to questions in this section. | Yes | 1 |
| CONN-1.1 Does the device support wireless connections? | No | |
| CONN-1.1.1 Does the device support Wi-Fi? (If yes, please list or provide reference to the Wi-Fi authentication protocols supported (e.g. WPA2 EAP-TLS) in the notes.) | N/A | |
| CONN-1.1.2 Does the device support Bluetooth? (If yes, please list or provide reference to the Bluetooth security modes supported and indicate if they can be forced in the notes.) | N/A | |
| CONN-1.1.3 Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)? (If yes, provide details or reference in notes.) | N/A | |
| CONN-1.1.4 Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? (If yes, provide details or reference in notes.) | N/A | |
| CONN-1.2 Does the device support physical connections? | Yes | 1 |
| CONN-1.2.1 Does the device have available RJ45 Ethernet ports? | Yes | 1 |
| CONN-1.2.2 Does the device have available USB ports? (If yes, provide details or reference that indicates use and how they are secured in notes.) | Yes | 3 |
| CONN-1.2.3 Does the device require, use, or support removable memory devices? (If yes, provide details or reference in notes.) | Yes | 2 |
| CONN-1.2.4 Does the device support other physical connectivity? (If yes, provide details or reference in notes.) | No | 1, 2 |
| CONN-2 Does the manufacturer provide a list of network ports and protocols that are used or may be used on the device? (If yes, provide details or reference in notes.) | Yes | 4 |
| CONN-3 Can the device communicate with other systems within the customer environment? (If yes, provide details or reference in notes.) | Yes | 1 |
| CONN-4 Can the device communicate with other systems external to the customer environment (e.g., a service host)? (If yes, provide details or reference in notes.) | No | |
| CONN-5 Does the device make or receive API calls? (If yes, provide details or reference in notes.) | No | |
| CONN-6 Does the device require an internet connection for its intended use? (If yes, provide details or reference in notes.) | No | |
| CONN-7 Does the device support Transport Layer Security (TLS)? (If yes, provide details or reference about supported and prohibited versions of TLS in the notes.) | No | 5 |
| CONN-7.1 Is TLS configurable? (If yes, provide details or reference in notes.) | No | |
| CONN-8 Does the device provide operator control functionality from a separate device (e.g., telemedicine)? (If yes, provide details or reference in notes.) | No | |

CONN notes:

1. LAN (RJ45) connection for DICOM connectivity is supported.
2. External USB drives are supported by the system.
3. Only specific items such as Software installation, system restore packages and service/DICOM licenses are read from external USB drives.
4. See Annex X
5. See DICOM conformance statement, available at http://siemens.com/DICOM

## SECURITY CAPABILITIES

| Refer to Section 2.3.15 of NEMA HN 1-2019 standard for the proper interpretation of information requested in this form. | Yes, No, N/A, or See Note | Note # |
|---|---|---|
| **12 PERSON AUTHENTICATION (PAUT)**<br>The ability to configure the **device** to authenticate **user**s | | |
| PAUT-1 Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)? | Yes | 1, 2 |
| PAUT-1.1 Does the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)? (If no, provide details or reference in notes.) | Yes | 1, 2, 3 |
| PAUT-2 Is the **device** configurable to authenticate **users** through an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, etc.)? (If yes, provide details or reference in notes.) | N/A | |
| PAUT-3 Is the device configurable to lock out a user after a certain number of unsuccessful logon attempts? (If yes, provide details or reference in notes.) | N/A | |
| PAUT-4 Are all default accounts (e.g., technician service accounts, administrator accounts) listed in the documentation? (If no, provide details or reference in notes.) | Yes | 7 |
| PAUT-5 Can all passwords be changed? (If no, provide details or reference in notes.) | Yes | |
| PAUT-6 Is the **device** configurable to enforce creation of **user** account passwords that meet established (organization specific) complexity rules? If so, provide details or reference in notes. | Yes | 4 |
| PAUT-7 Does the device support account passwords that expire periodically? (If yes, provide details or reference in notes.) | Yes | 4 |
| PAUT-8 Does the device support multi-factor authentication? (If yes, provide details or reference in notes.) | No | |
| PAUT-9 Does the device support single sign-on (SSO)? (If yes, provide details or reference in notes.) | No | |
| PAUT-10 Can user accounts be disabled/locked on the device? | Yes | 1 |
| 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? (If so, provide details or reference in notes.) | Yes | 1, 5 |
| PAUT-14.1 Are credentials stored using a secure method? (If so, provide details or reference in notes.) | N/A | 6 |

PAUT notes:

1. Available when user management is turned On.
2. Service user access is access controlled with time-based service licenses
3. Emergency user is not access controlled.
4. See Operator Manual.
5. The system stores authentication credentials locally on an SD card located inside the system covers.
6. Authentication credentials are hashed and stored.
7. See Annex V.

| **13 PHYSICAL LOCKS (PLOK)**<br>Physical locks can prevent unauthorized **users** with physical access to the **device** from compromising the integrity and confidentiality of **personally identifiable information** stored on the **device** or on **removable media**. | | |
|---|---|---|
| PLOK-1 Is the device software only? (If yes, answer "N/A" to remaining questions in this section.) | No | |
| PLOK-2 Are all **device** components maintaining **personally identifiable information** (other than **removable media**) physically secure (i.e., cannot remove without tools)? | Yes | 1 |
| PLOK-3 Are all **device** components maintaining **personally identifiable information** (other than **removable media**) physically secured behind an individually keyed locking device? | No | |
| PLOK-4 Does the device have an option for the customer to attach a physical lock to restrict access to removable media? | No | |

PLOK notes:

1. Siemens Healthineers recommends running the device in an environment where only authorized personnel have access to the devices.

## SECURITY CAPABILITIES

| Refer to Section 2.3.17 of NEMA HN 1-2019 standard for the proper interpretation of information requested in this form. | Yes, No, N/A, or See Note | Note # |
|---|---|---|
| **14 ROADMAP FOR THIRD PARTY APPLICATIONS AND SOFTWARE COMPONENTS IN DEVICE LIFE CYCLE (RDMP)** Manufacturer's plans for security support of third-party applications and software components, including custom components, within the device's life cycle, such as how third-party End of Life will be managed. | | |
| RDMP-1 Was a secure software development process, such as ISO/IEC 27034 or IEC 62304, followed during product development? (If yes, provide details or reference in notes.) | Yes | 3 |
| 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? (If yes, provide details or reference in notes.) | Yes | 1 |
| RDMP-4 Does the manufacturer have a plan for managing third-party component end-of-life? (If yes, provide details or reference in notes.) | Yes | 2 |
| RDMP notes: 1. See Annex W 2. Regular and critical updates provided as per patching strategy. 3. The system is developed in accordance with requirements which have been derived and mapped to Secure in Use standards like CLSI Auto11-A2, IEC TR 80001-2-2, IEC TR 80001-2-8, ANSI/NEMA HN 1-2019 (MDS²). The already available SHS guidance documents (SHS Basics Data Protection Products) are incorporated. In addition, the system requirements have been compared and mapped to general accepted industry standards like IEC 62443-3-3, IEC 62443-4-2, BSI 132 or open-source IT security guidelines (provided by the Johner Institute in close collaboration with Tüv Süd). | | |
| **15 SOFTWARE BILL OF MATERIALS (SBOM)** A Software Bill of Material (SBoM) lists all the software components that are incorporated into the device being described for the purpose of operational security planning by the healthcare delivery organization. This section supports controls in the RDMP section. | | |
| SBOM-1 Is the SBoM for this product available? (If yes, provide details or reference in notes.) | Yes | 1 |
| SBOM-2 Does the SBoM follow a standard or common method in describing software components? (If yes, provide details or reference in notes.) | No | |
| 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? (If yes, provide details or reference in notes.) | Yes | 2 |
| SBOM-3 Does the device include a command or process method available to generate a list of software components installed on the device? (If yes, provide details or reference in notes.) | Yes | 3 |
| SBOM-4 Is there an update process for the SBoM? (If yes, provide details or reference in notes.) | Yes | 3 |
| SBOM notes: 1. See Annex W 2. Software license clearing has been done. 3. SBoM process is followed to provide the OSS software via a DVD. | | |

## SECURITY CAPABILITIES

| Refer to Section 2.3.19 and following of NEMA HN 1-2019 standard for the proper interpretation of information requested in this form. | Yes, No, N/A, or See Note | Note # |
|---|---|---|
| 16 SYSTEM AND APPLICATION HARDENING (SAHD)<br>The device's inherent resistance to cyber-attacks and malware. | | |
| SAHD-1 Is the **device** hardened in accordance with any industry standards? (If yes, provide details or reference in notes.) | Yes | 1 |
| SAHD-2 Has the device received any cybersecurity certifications? (If yes, provide details or reference in notes.) ..... | No | |
| SAHD-3 Does the device employ any mechanisms for software integrity checking? ..... | Yes | 2 |
| 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 | 2 |
| SAHD-3.2 Does the **device** employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the software updates are the manufacturer-authorized updates? | Yes | 2 |
| SAHD-4 Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)? (If yes, provide details or reference in notes.) ..... | No | |
| SAHD-5 Is the system configurable to allow the implementation of file-level, patient level, or other types of access controls? (If yes, provide details or reference in notes.) ..... | Yes | 3, 4 |
| SAHD-5.1 Does the device provide role-based access controls? ..... | Yes | 3. 4 |
| SAHD-6 Are any system or user accounts restricted or disabled by the manufacturer at system delivery? If yes, provide details or reference in notes. ..... | Yes | 3 |
| SAHD-6.1 Are any system or user accounts configurable by the end user after initial configuration? ..... | Yes | |
| SAHD-6.2 Does this include restricting certain system or user accounts, such as service technicians, to least privileged access? ..... | No | |
| SAHD-7 Are all shared resources (e.g., file shares) which are not required for the **intended use** of the **device** disabled? (If yes, provide details or reference in notes.) ..... | N/A | |
| SAHD-8 Are all communication ports and protocols that are not required for the **intended use** of the **device** disabled? (If yes, provide details or reference in notes.) ..... | Yes | 5, 6, 7 |
| 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? (If yes, provide details or reference in notes.) ..... | Yes | 8 |
| 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? (If yes, provide details or reference in notes.) | Yes | 9 |
| SAHD-11 Can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)? (If yes, provide details or reference in notes.) ..... | Yes | 6 |
| SAHD-12 Can unauthorized software or hardware be installed on the **device** without the use of physical tools? If yes, provide details or reference in notes. ..... | No | |
| SAHD-13 Does the product documentation include information on operational network security scanning by users? (If yes, provide details or reference in notes.) ..... | Yes | 8, 9 |
| SAHD-14 Can the device be hardened beyond the default provided state? ..... | No | |
| SAHD-14.1 Are instructions available from vendor for increased hardening? (If yes, provide details or reference in notes.) ..... | No | |
| SAHD-15 Can the system prevent access to BIOS or other bootloaders during boot? ..... | Yes | 6 |
| SAHD-16 Have additional hardening methods not included in **SAHD** been used to harden the device? (If yes, provide details or reference in notes.) ..... | No | |

SAHD notes:

1. The system is developed in accordance with requirements which have been derived and mapped to Secure in Use standards like CLSI Auto11-A2, IEC TR 80001-2-2, IEC TR 80001-2-8, ANSI/NEMA HN 1-2019 (MDS²). The already available SHS guidance documents (SHS Basics Data Protection Products) are incorporated. In addition, the system requirements have been compared and mapped to general accepted industry standards like IEC 62443-3-3, IEC 62443-4-2, BSI 132 or open-source IT security guidelines (provided by the Johner Institute in close collaboration with Tüv Süd).
2. User management needs to be turned on. User Management is disabled by default and needs to be turned on by CSE on request of Customer.
3. Service user access is access controlled with time-based service licenses
4. Firewall is active with dedicated inbound rules. Only needed ports are open. (see Annex X for a list of open ports)
5. USB boot is disabled.
6. Only DICOM ports are open.
7. A list of enabled services is provided in Annex Y – 1 and Annex Y – 2.
8. It is strictly recommended **not** to perform non-instrumented network security scans in parallel to the clinical use of the system.

## SECURITY CAPABILITIES

| Refer to Section 2.3.19 and following of NEMA HN 1-2019 standard for the proper interpretation of information requested in this form. | Yes, No, N/A, or See Note | Note # |
|---|---|---|
| **17 SECURITY GUIDANCE (SGUD)**<br>The availability of security guidance for **operator** and administrator of the system and manufacturer sales and service. | | |
| SGUD-1 Does the device include security documentation for the owner/operator? (If yes, provide details or reference in notes.) | Yes | 1 |
| SGUD-2 Does the device have the capability, and provide instructions, for the permanent deletion of data from the device or media? (If yes, provide details or reference in notes.) | Yes | 2, 3 |
| SGUD-3 Are all access accounts documented? | Yes | 4, 5 |
| SGUD-3.1 Can the owner/operator manage password control for all accounts? | Yes | 4, 5 |
| SGUD-4 Does the product include documentation on recommended compensating controls for the device? | N/A | |

SGUD notes:

1. See Operator Manual.
2. Instruction (Disposal Instruction) for the Siemens Service Technician that the SD card with sensitive data must be handed over to the hospital.
3. Instruction (Replacement of Parts) for the Siemens Service Technician for the SD Card to be swapped with the new SD Card to avoid patient data loss or misuse.
4. Available when user management is turned On. See Annex V.
5. Service user access is access controlled with time-based service licenses.

| **18 DATA STORAGE CONFIDENTIALITY (STCF)**<br>The ability of the device to ensure unauthorized access does not compromise the integrity and confidentiality of personally identifiable information and other protected personal information (PPI) stored on device or removable media. | | |
|---|---|---|
| STCF-1 Can the **device** encrypt data at rest? (If yes, provide details or reference in notes.) | No | |
| STCF-1.1 Is all data encrypted or otherwise protected? (If yes, describe or provide a reference in notes.) | N/A | |
| STCF-1.2 Is the data encryption capability configured by default? | N/A | |
| STCF-1.3 Are instructions available to the customer to configure encryption? | N/A | |
| STCF-2 Can the encryption keys be changed or configured? (If yes, describe or provide a reference in notes.) | N/A | |
| STCF-3 Is the data stored in a database located on the device? (If yes, describe or provide a reference in notes.) | Yes | 1 |
| STCF-4 Is the data stored in a database external to the device? (If yes, describe or provide a reference in notes.) | No | 1 |

STCF notes:

1. Patient data is stored on an SD card located inside the system covers.

| 19 TRANSMISSION CONFIDENTIALITY (TXCF)<br>The ability of the device to ensure the confidentiality of transmitted personally identifiable information. | | |
|---|---|---|
| TXCF-1 Can **personally identifiable information.** be transmitted only via a point-to-point dedicated cable? | Yes | 1 |
| TXCF-2 Is **personally identifiable information.** encrypted prior to transmission via a network or **removable media**? (If yes, indicate in the notes which encryption standard is implemented.) | No | |
| TXCF-2.1 If data is not encrypted by default, can the customer configure encryption options? | N/A | |
| TXCF-3 Is **personally identifiable information** transmission restricted to a fixed list of network destinations? | Yes | 2 |
| TXCF-4 Are connections limited to authenticated systems? If yes, describe or provide a reference in notes. | Yes | 2 |
| TXCF-5 Are secure transmission methods supported/implemented (DICOM, HL7, IEEE 11073)? (If yes, describe or provide a reference in notes.) | No | |

TXCF notes:

1. LAN (RJ45) connection for DICOM connectivity is supported.
2. DICOM operations are restricted to configured network nodes.

## SECURITY CAPABILITIES

| Refer to Section 2.3.21 and following of NEMA HN 1-2019 standard for the proper interpretation of information requested in this form. | Yes, No, N/A, or See Note | Note # |
|---|---|---|
| **20 TRANSMISSION INTEGRITY (TXIG)**<br>The ability of the **device** to ensure the integrity of transmitted **data**. | | |
| TXIG-1 Does the **device** support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission? (If yes, describe or provide a reference in notes.) ..... | No | 1 |
| TXIG-2 Does the device include multiple sub-components connected by external cables? If yes, describe or provide a reference in notes. ..... | No | 2 |

TXIG notes:
1. DICOM Storage Commitment protocol to ensure that receiver takes responsibility of DICOM data transmitted.
2. C arm is connected to the Trolley with the **Monitor-cart connection cable**.

| **21 REMOTE SERVICE (RMOT)**<br>Remote service refers to all types of device maintenance activities performed by a service person via network or other remote connection. | | |
|---|---|---|
| RMOT-1 Does the device permit remote service connections for device analysis or repair? (If yes, describe or provide a reference in notes.) ..... | No | |
| RMOT-1.1 Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair? | N/A | |
| RMOT-1.2 Is there an indicator for an enabled and active remote session? ..... | N/A | |
| RMOT-1.3 Can patient data be accessed or viewed from the device during the remote session?..... | N/A | |
| RMOT-2 Does the device permit or use remote service connections for predictive maintenance data? (If yes, describe or provide a reference in notes.) ..... | No | |
| RMOT-3 Does the device have any other remotely accessible functionality (e.g. software updates, remote training)? (If yes, describe or provide a reference in notes.)..... | No | |

RMOT notes:

| **22 OTHER SECURITY CONSIDERATIONS (OTHR)**<br>This section should be populated by the manufacturer with security risk considerations or controls (including compensating controls) that have not been categorized elsewhere in this document. | | |
|---|---|---|
| OTHR-1 General consideration to be observed | See Note | 1 |

OTHR notes:

1. It is strictly recommended **not** to perform non-instrumented network security scans in parallel to the clinical use of the system.

RECOMMENDED SECURITY PRACTICES

- Siemens Healthineers products are prepared to be operated in a secure environment. If the local network is operated by the customer, it is his responsibility to ensure the required level of security, e.g. perform client authentication of devices connected to the network
- This device is designed to be operated in a protected network environment. Siemens Healthineers advises against directly connecting the device to public networks
- Comprehensive recommendations how customers can defend their Medical IT Systems against malicious attacks are given in the NEMA approved White Paper "Defending Medical Information Systems against Malicious Logic" available on www.nema.org/medical/spc.

The configuration of the product should follow the product specific instructions for use and need to take into account the local conditions

| Annex U – Cybersecurity - Auditing | |
|---|---|
| **Does the proposed medical system/device support any of the following?** | **Primary Application** |
| Audit logs | Yes |
| Retention settings for system logs | No |
| Audit logs protection from deletion | Yes |
| Audit reduction capability that supports on-demand audit review and analysis? | No |
| Audit reduction capability that supports after-the-fact investigations of security incidents? | No |
| Audit reduction capability that does not alter original content or time ordering of audit records? | Yes |
| Are audit trail events date/time stamped? | Yes |
| Are audit trail events date/time stamped that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT)? | No |
| Can audit trail events include source/destination IP information? | No |
| Can audit trail events include protocols? | Yes |
| Can audit trail events include User ID information? | Yes |
| Can audit trail events include changes to Administrator account information? | Yes |
| Can audit trail events include login/logout information? | Yes |
| Can audit trail events include the display/presentation of data? | No |
| Can audit trail events include the creation, modification and deletion of data? | Yes |
| Can audit trail events include the import and export of data to and from removable media? | Yes |
| Can audit trail events include the receipt and transmission of data with external (e.g. network) connections? | Yes |
| Can audit trail events include Remote Service activity? | No |
| Can audit trail events include the logging of the execution of privileged functions? | Yes |

| Annex V – List of User Accounts | | | | |
|---|---|---|---|---|
| **Account Name** | **Authentication provided by:**<br>- Local<br>- Active Directory<br>- Other | **Characteristics:**<br>- Level of OS permissions (admin vs. non-admin)<br>- Used for auto-login | **Password**<br>Is it configurable?<br>Is it hardcoded?<br>Is it resettable? | **Purpose / Notes** |
| N/A | N/A | N/A | N/A | N/A |

Notes:

1. Clinical user accounts are available only when user management is turned On (by the CSE).
2. The **first system administrator** account **is created by the CSE post system installation**.
3. The first system administrator account password can be reset only by self or the CSE.
4. The first system administrator account cannot be deleted.
5. Administrative privileges for the first system administrator account cannot be removed.
6. The other system administrator account passwords can be reset by self or a system administrator.
7. Clinical user account privileges can be assigned/removed by the system administrator.
8. Administrative privileges can be assigned/removed by the system administrator.
9. Maintenance of audit logs (export/delete) is done by the system administrator.
10. No predefined user accounts delivered with system.
11. Service user access is access controlled with time-based service licenses.

| Annex W – List of (3rd party) Applications | | | |
|---|---|---|---|
| **Application Name** | **Version #** | **Running on Asset** | **Purpose / comment** |
| Linux | 3.14 | Cios Fit | Operating system for the product |
| Qt | 5.6 | Cios Fit | Framework for Graphical User Interface |
| SQLite | 3.28 | Cios Fit | Patient Database |
| Printer driver | 1.4.0 | Cios Fit | Sony printer driver |
| Merge DICOM toolkit | 5.3 | Cios Fit | DICOM toolkit |

Note:
This table lists relevant third-party technologies used. A comprehensive list is maintained on **teamplay Fleet*** (**https://fleet.siemens-healthineers.com/welcome**)
** For supported countries, this requires a customer account in teamplay Fleet. Please contact your local Siemens Healthineers organization for further details.*

| Annex X – List of opened Ports | | | | |
|---|---|---|---|---|
| **Protocol / Services used** | **TCP / UDP** | **Port #** | **Inbound/ Outbound** | **Notes / Description** |
| HIS / RIS (DICOM) | TCP | User configured | Inbound Outbound | Used to query and receive DICOM Worklist Data from HIS/RIS |
| PRINT (DICOM) | TCP | User configured | Inbound Outbound | Used for DICOM print operations |
| PACS (DICOM) | TCP | User configured | Inbound Outbound | Used to receive images from other Systems (e.g. PACS) |

Note:

1. The below ports are blocked:
    a. TCP - 21
    b. TCP - 22
    c. TCP - 3002
    d. TCP - 35347
    e. UDP - 5353
2. All connections except the user-configured DICOM ports are blocked.

**Annex Y – 1 – List of running services – Main Processor**

- init
- kthreadd
- ksoftirqd/0
- kworker/0:0H
- rcu_preempt
- rcu_sched
- rcu_bh
- migration/0
- migration/1
- ksoftirqd/1
- kworker/1:0
- kworker/1:0H
- migration/2
- ksoftirqd/2
- kworker/2:0H
- migration/3
- ksoftirqd/3
- kworker/3:0
- kworker/3:0H
- khelper
- kdevtmpfs
- writeback
- bioset
- crypto
- kblockd
- ata_sff
- ipu1_task
- ipu2_task
- cfinteractive
- kworker/0:1
- kswapd0
- fsnotify_mark
- kworker/0:2
- scsi_eh_0
- scsi_tmf_0
- spi0
- irq/192-2198000
- kworker/3:1
- vpu_wq
- deferwq
- irq/81-imx_ther
- mmcqd/2
- kworker/1:1
- mmcqd/3
- mmcqd/3boot0
- mmcqd/3boot1
- mmcqd/3rpmb
- kworker/0:1H
- jbd2/mmcblk3p3-
- ext4-rsv-conver
- kworker/2:1
- /sbin/syslogd
- /sbin/klogd
- jbd2/mmcblk3p6-
- kworker/3:1H
- jbd2/mmcblk3p7-
- /usr/sbin/dropbear
- irisd
- collimatord
- /sbin/udevd
- kworker/2:1H
- galcore workque
- kworker/1:1H
- khubd
- Vivante Kernel
- jbd2/mmcblk2p1-
- galcore daemon
- dbus-daemon
- kworker/2:2
- /usr/sbin/cupsd
- /usr/lib/cups/notifier/dbus
- /usr/sbin/cups-browsed
- /sbin/getty
- ./icmp
- {start_S34DUIApp}
- ./S34DUIApp
- {dropCache.sh}
- ./canadapter
- /XCU_ROOT/BIN/axnroot
- ./Monitor
- candump
- /XCU_ROOT/BIN/XCU_2
- irq/384-ad7924_
- AafStdParser
- /XCU_ROOT/BIN/DCU
- sleep
- kworker/u8:2
- kworker/u8:5

**Annex Y – 2 – List of running services – Co Processor**

- init
- kthreadd
- ksoftirqd/0
- kworker/0:0
- kworker/0:0H
- kworker/u8:0
- rcu_preempt
- rcu_sched
- rcu_bh
- migration/0
- migration/1
- ksoftirqd/1
- kworker/1:0
- kworker/1:0H
- migration/2
- ksoftirqd/2
- kworker/2:0
- kworker/2:0H
- migration/3
- ksoftirqd/3
- kworker/3:0
- kworker/3:0H
- khelper
- kdevtmpfs
- writeback
- bioset
- crypto
- kblockd
- ata_sff
- ipu1_task
- ipu1_task
- ipu2_task
- ipu2_task
- cfinteractive
- kworker/0:1
- kswapd0
- fsnotify_mark
- kworker/1:1
- scsi_eh_0
- scsi_tmf_0
- spi0
- kworker/u8:2
- kworker/2:1
- irq/192-2198000
- vpu_wq
- mmcqd/3
- mmcqd/3boot0
- mmcqd/3boot1
- mmcqd/3rpmb
- deferwq
- kworker/3:1
- irq/81-imx_ther
- kworker/0:1H
- jbd2/mmcblk3p3-
- ext4-rsv-conver
- /sbin/syslogd
- /sbin/klogd
- jbd2/mmcblk3p6-
- ext4-rsv-conver
- jbd2/mmcblk3p7-
- ext4-rsv-conver
- /usr/sbin/dropbear
- /sbin/udevd
- kworker/1:1H
- galcore workque
- kworker/2:1H
- Vivante Kernel
- galcore daemon
- galcore daemon
- galcore daemon
- dbus-daemon
- /sbin/getty
- /root/app/tools/wdd
- {iccp Consumer}
- /usr/sbin/dropbear

## Annex Z – STATEMENT ACCORDING TO IEC 60601-1:2012; Edition 3.1, sub-clause 14.13

### Z1 Instructions for the responsible Organization

| | |
|---|---|
| Z1-1 | Connection of the system to a NETWORK / DATA COUPLING that includes other equipment could result in previously unidentified risks to patients, operators or third parties;<br>the RESPONSIBLE ORGANIZATION should identify, evaluate and control these risks |
| Z1-2 | Subsequent changes to the NETWORK / DATA COUPLING could introduce new RISKS and require additional analysis. |
| Z1-3 | Changes to the network include:<br>- changes in NETWORK / DATA COUPLING configuration;<br>- connection to additional items to the NETWORK / DATA COUPLING;<br>- disconnecting items from the NETWORK / DATA COUPLING;<br>- update of equipment connected to the NETWORK / DATA COUPLING;<br>- upgrade of equipment connected to the NETWORK / DATA COUPLING; |
| Z1 notes: | "Cybersecurity Conditions Healthcare" (see "Terms & Conditions") applies.<br>See "Intended operational environment". |

### Z2 Intended purpose of integrating the Device into an IT-Network

| | |
|---|---|
| Z2-1 | The Siemens Healthineers Cios Fit is designed as a mobile C-arm. |
| Z2-2 | The system consists of the following components: |
| Z2-2.1 | C-arm (main unit) with X-ray tube, X-ray detector and X-ray generator. |
| Z2-2.2 | Monitor cart with a touch-monitor and a (optional) printer. |
| Z2-3 | The system is DICOM compliant, allowing it to be connected to a network with other compliant devices for the exchange of images. Networking allows transmission of images acquired to other DICOM compatible review stations or PACS. A list of all patients ever imaged can be kept on the Radiology PACS making future retrievals fast and easy. |
| Z2-4 | The system connects to the network through an Ethernet cable. The network interface allows DICOM connections to specific clinical systems such as a Radiology PACS, console workstation image viewer, or printer. Patient demographic data will be received via DICOM, acquired images will be sent to the Radiology PACS or DICOM workstations via hardwired connection only for detailed viewing and long-term storage. |
| Z2-5 | The system provides a Third-Party Software Interface which enables Third Parties to exchange data with the system. The Third Party Software Interface uses encrypted AMQP communication protocol to exchange data (e.g. table position, Patient data). **– N/A for Cios Fit** |
| Z2-6 | The system provides Remote Assist functionality, which enables the user gathering support from other systems in the IT-Network. **– N/A for Cios Fit** |
| Z2 notes: | "Cybersecurity Conditions Healthcare" (see "Terms & Conditions") applies.<br>See "Intended operational environment". |

### Z3 Network Properties required by the System and resulting risks

| | |
|---|---|
| Z3-1 | Ethernet Connection of the clinical Network (TCP/IP, 1Gbit/s) |
| Z3-1.1 | If the network is down the network services (see below) is not available which can lead to the risks stated below. |
| Z3-1.2 | If the network is unavailable, medical images cannot be transferred for remote consultation. |
| Z3-1.3 | If the recommended network performance (1Gbit/s) is not provided, the transfer of images is extended and availability of images at destinations (e.g. for consulting) is delayed. |
| Z3-1.4 | If the direct access to the System from the Internet is generally possible through the clinical network (e.g. no firewall is provided), the existing protection mechanisms can be exploited by an experienced hacker and the proper system operation can no longer be guaranteed. |
| Z3-1.5 | Performing network security scans or controlled penetration test of the System during a running medical procedure can lead to unavailability of necessary network services (see below) needed to complete the medical procedure. |
| Z3-2 | PACS system for archiving of Images |
| Z3-2.1 | If the PACS is not available, images cannot be archived after the examination. In case of a system hardware failure all not archived images can be lost. |
| Z3-2.2 | If the PACS is not available, images cannot be archived after the examination. Examinations may overwrite data because disk is full (because older images are automatically overwritten). |
| Z3-2.3 | If the PACS is not available, images cannot be archived after the examination. In case of manual deletion of images, not archived images can be lost. |
| Z3-2.4 | If the PACS is not available, images are not available for remote consultation via PACS consoles. |
| Z3-2.5 | If the PACS is not available, prior images are not available. |

| | |
|---|---|
| Z3-2.6 | If the recommended network performance (1Gbit/s) is not provided, the transfer time to PACS is extended and the time to wait before switching off the System consecutive to last transfer operations is prolonged. |
| Z3-3 | DICOM Printer |
| Z3-3.1 | If the DICOM printer is not available, film is not available for diagnose/archive. |
| Z3-4 | RIS System |
| Z3-4.1 | If the RIS system is not available, modality worklist is not available. This can lead to data inconsistencies. |
| Z3-4-2 | If the RIS system is not available, modality worklist is not available. This can lead to images sent to the PACS are possibly not available until manually coerced with the RIS data in the PACS. **– N/A for Cios Fit** |
| Z3-4.3 | If case a reduced network performance shall be compensated by a long Worklist Query time-out, this results in the possibility that non-actual RIS data are used when registering a patient from the list of schedules on the System. |
| Z3-5 | Network Connection to Siemens Remote Service Server. **– N/A for Cios Fit** |
| Z3-5.1 | If the connection to the Remote Service Server is not available, SW patches cannot be distributed. **– N/A for Cios Fit** |
| Z3-5.2 | If the connection to the Remote Service Server is not available, SIEMENS Support is restricted. **– N/A for Cios Fit** |
| Z3-6 | Network Connection to Third Party Software Interface. **– N/A for Cios Fit** |
| Z3-6.1 | If the connection to the Third-Party Software Interface is not available, the corresponding Third Party Application will not be able to receive required Data. **– N/A for Cios Fit** |
| Z3 notes: | N/A |

# Abbreviations

| | |
|---|---|
| AD | Active Directory |
| AES | Advanced Encryption Standard |
| BIOS | Basic Input Output System |
| BOM | Bill Of Materials |
| CSE | Customer Service Engineer |
| DES | Data Encryption Standard |
| DICOM | Digital Imaging and Communications in Medicine |
| 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 |
| IDS | Intrusion Detection System |
| IEC | International Electrotechnical Commission |
| IPS | Intrusion Prevention System |
| IVM | Intervention Module |
| LDAP | Lightweight Directory Access Protocol |
| MD5 | Message Digest 5 |
| MDS2 | Manufacturer Disclosure Statement for Medical Device Security |
| MSTS | Microsoft Terminal Server |
| NEMA | National Electrical Manufacturers Association |
| NTP | Network Time Protocol |
| OCR | Office for Civil Rights |
| OU | Organizational Unit |
| PACS | Picture Archiving and Communication System |
| PHI | Protected Health Information |
| PII | Personally Identifiable Information |
| RIS | Radiology Information System |
| RPC | Remote Procedure Call |
| RSA | Random Sequential Adsorption |
| SAM | Security Accounts Manager |
| SHA | Secure Hash Algorithm |
| SIEM | Security Information and Event Management |
| SOP | Standard Operating Procedure |
| SQL | Structured Query Language |
| SRS | (Siemens) Smart Remote Services |
| SVP | Security Vulnerability Patch |
| SW | Software |
| TCP | Transmission Control Protocol |
| UDP | User Datagram Protocol |
| VPN | Virtual Private Network |

# Disclaimer according to IEC 80001-1

- 1-1 The Device has the capability to be connected to a medical IT-network which is managed under full responsibility of the operating responsible organization. It is assumed that the responsible organization assigns a Medical IT-Network Risk Manager to perform IT-Risk Management (see IEC 80001- 1:2010/EN 80001-1:2011) for IT-networks incorporating medical devices.
- 1-2 This statement describes Device-specific 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 like e.g. malware or denial-of-service.
- 1-5 Unintended consequences (like e.g. misuse/loss/corruption) of data not under control of the Device e.g. after electronic communication from the Device to some IT-network or to some storage, are under the responsibility of the responsible organization.
- 1-6 Unauthorized use of the external connections or storage media of the Device can cause hazards regarding the availability and information security of all components of the medical IT-network. The responsible organization must ensure – through technical and/or organizational measures - that only authorized use of the external connections and storage media is permitted.

**International Electrotechnical Commission Glossary (extract)**

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

# Statement on FDA Cybersecurity Guidance

Cios Fit is not available in the USA.

*Order No. A91AT-40020-22T3-7600 · Print No. ATSC-100.640.02.01.02 · SAP 11250737-ESK-01S-03*
*Published by Siemens Healthcare GmbH ·* 

On account of certain regional limitations of sales rights and service availability, we cannot guarantee that all products included in this brochure are available through the Siemens sales organization worldwide. Availability and packaging may vary by country and are subject to change without prior notice.

Some/All of the features and products described herein may not be available in the United States or other countries.

The information in this document contains general technical descriptions of specifications and options as well as standard and optional features that do not always have to be present in individual cases.

Siemens reserves the right to modify the design, packaging, specifications and options described herein without prior notice. Please contact your local Siemens sales representative for the most current information.

In the interest of complying with legal requirements concerning the environmental compatibility of our products (protection of natural resources and waste conservation), we recycle certain components. Using the same extensive quality assurance measures as for factory-new components, we guarantee the quality of these recycled components.

Note: Any technical data contained in this document may vary within defined tolerances. Original images always lose a certain amount of detail when reproduced.

Caution: Federal law restricts this device to sale by or on the order of a physician.

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

**Manufacturer**
Siemens Healthcare Private Limited
Unit No. 9A, 9th Floor, North Tower,
Godrej One, Pirojshanagar
Vikroli East, Mumbai – 400079
India

*Order No. A91AT-40020-22T3-7600 · Print No. ATSC-100.640.02.01.02 · SAP 11250737-ESK-01S-03*
*Published by Siemens Healthcare GmbH · © Siemens Healthcare GmbH, 2022*