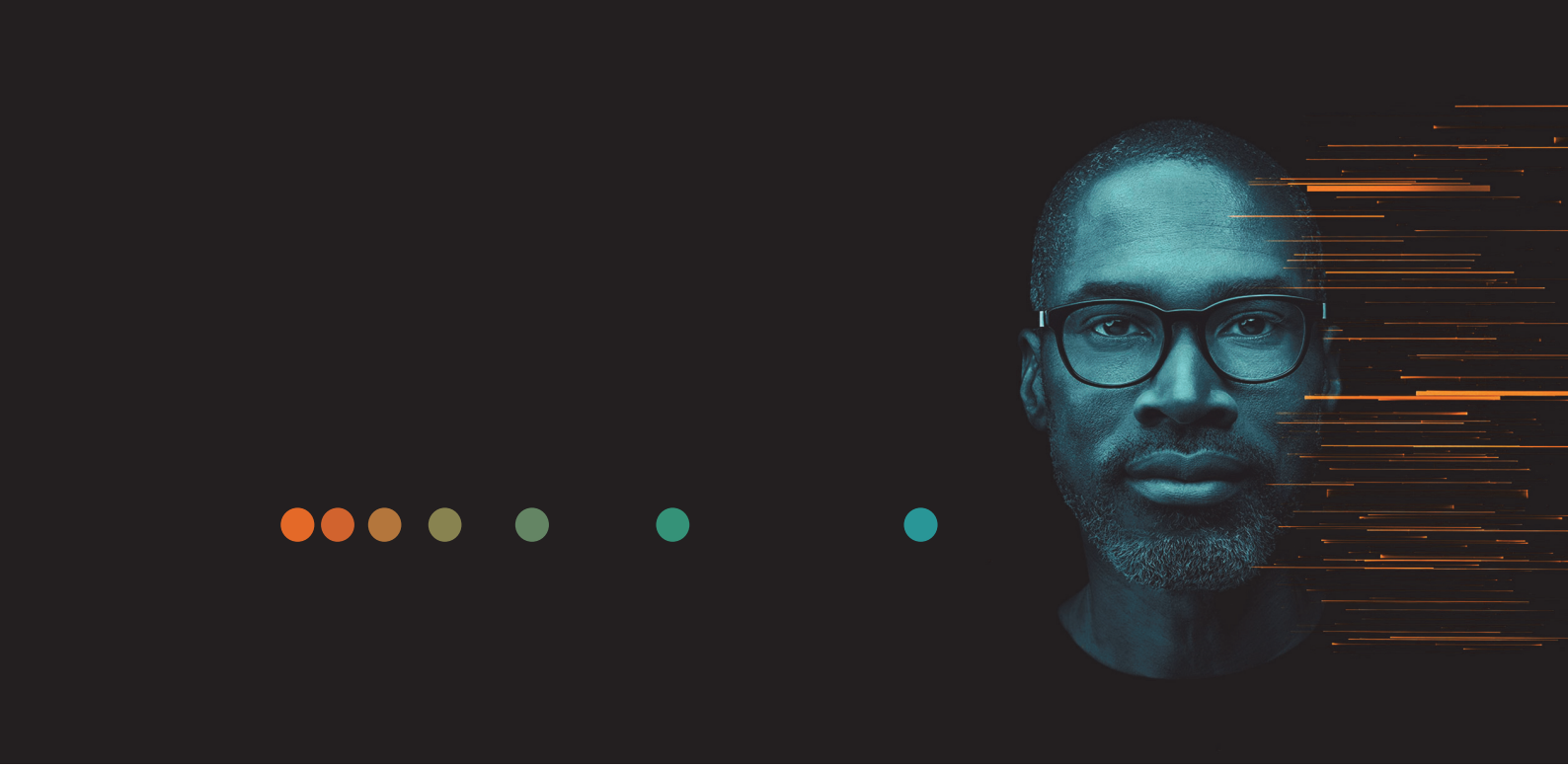


Whitepaper

syngo MR XA50 security whitepaper

The facts about the security of our products and solutions.

siemens-healthineers.com/cybersecurity

SIEMENS Healthineers

Foreword

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

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

We comply with applicable security and privacy laws and will cooperate with the competent authorities including, but not limited to, the US Department of Health and Human Services (HHS), the US Food and Drug Administration (FDA), the US Office for Civil Rights (OCR), the EU General Data Protection Regulation (GDPR), the National Medical Products Administration (NMPA) in China, and the EU Medical Device Regulation (MDR) to meet IT security and privacy obligations.

Vulnerability and incident management
Siemens Healthineers cooperates with government agencies and cybersecurity researchers concerning reported potential vulnerabilities. Our communications policy strives for coordinated disclosure. We work in this way with our customers and other parties, when appropriate, in response to potential vulnerabilities and incidents in our products, no matter 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 products
- Incorporating secure architecture, design and coding methodologies in our software development process
- Performing static code analysis of our products
- Conducting security testing of products under development as well as products already in the field
- Providing a patch management strategy for the medical device
- Monitoring security vulnerabilities to track reported third party component issues in our products
- Working with suppliers to address security throughout the supply chain
- Training of employees to provide knowledge consistent with their level of responsibility 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

Jim Jacobson
Chief Product and Solution Security Officer
Siemens Healthineers

Contents

Basic information

The MAGNETOM systems are magnetic resonance imaging (MRI) devices that produce transverse, sagittal, coronal and oblique cross-sectional images, spectroscopic images and/or spectra, and display the internal structure and/or function of the head, body, or extremities. To generate clinically relevant images MRI systems include the following main components/subsystems:
- a magnet with a main magnetic field,
- a gradient system,
- the radio-frequency system and
- a computer system incl. dedicated software

Operating systems

- *syngo* MR XA50 software is based on Microsoft Windows 10 Enterprise

For more information about the software installed please refer to the Software Bill of Material chapter.

User account information

- *syngo* MR XA50 supports HIPAA (Health InsurancePortability and Accountability Act) regulation with role-based privilege assignment and access control.
- The system provides preconfigured password policies which can be customized by administrators.
- More information is provided in the administration manual.

Default passwords

The standard accounts are provided with factory default passwords. For security reasons, it is recommended to change the password during installation. The same applies to the BIOS password.
The customer is responsible for storing the passwords in a secure manner and making the passwords available to Siemens Healthineers Customer Services, if necessary.

Patching strategy

The MAGNETOM system is a medical device that consists of hardware and software. All third-party software, including the operating system, belongs to the medical device. All software updates and patches are first evaluated by the vendor before they are released in order to make sure that there are no adverse effects to safety and essential performance. Siemens Healthineers strongly discourages customers from modifying the software without consent by the vendor since this will violate the certification of the system as a medical device.
Siemens Healthineers strives to deliver the system free of any vulnerabilities that are known at the time of delivery. No unacceptable risks due to known vulnerabilities are assumed to be present when the system is delivered to the customer.
Siemens Healthineers continuously monitors used third-party software (including operating system) for vulnerabilities and assesses the severity using the CVSS model. For vulnerabilities with unacceptable risks, patches (called “security deliveries”) are published on a regular basis.

Cryptography usage

- *syngo* MR XA50 utilizes ciphers and protocols built into Windows 10 for encryption and data protection. Hardening measures limit the usage to those which are at least FIPS 140 compliant.
- TLS is used for:
  - DICOM encryption
  - HTTPS connection for Smart Remote Services
- SHA-2 is used for digital signature of the binaries
  in the context of whitelisting
- Microsoft Windows® User Management

Handling of sensitive data

- Protected Health Information (PHI) is stored on the MRI system (Digital Imaging and Communication in Medicine (DICOM) data, raw data, meta data for DICOM creation).
- PHI is transmitted via DICOM (configurable: encrypted/unencrypted).
- The MRI system is designed for temporary data storage of PHI data only. Siemens Healthineers recommends storing respective data to a long-term archive, e.g. on a Picture Archiving and Communication System (PACS) and to subsequently delete the data on the MRI system by customer defined procedures.
- PHI and PII data in audit trail are supported according to the Health Insurance Portability and Accountability Act (HIPAA).
- Personally Identifiable Information (PII) as part of the DICOM records or in log files is also stored on the MRI system, e.g., names, personal identifier, account names.
- Additional sensitive information might be present in user editable input fields or in the acquired images.

Data recovery
It is assumed that PHI is archived to a PACS after the patient scan was completed or images/reports are ready after postprocessing.
The system supports backup and restoration of system configuration to an external drive.
The device is not intended to provide any backup mechanism for imaging and reporting, which may contain PHI or PII data.

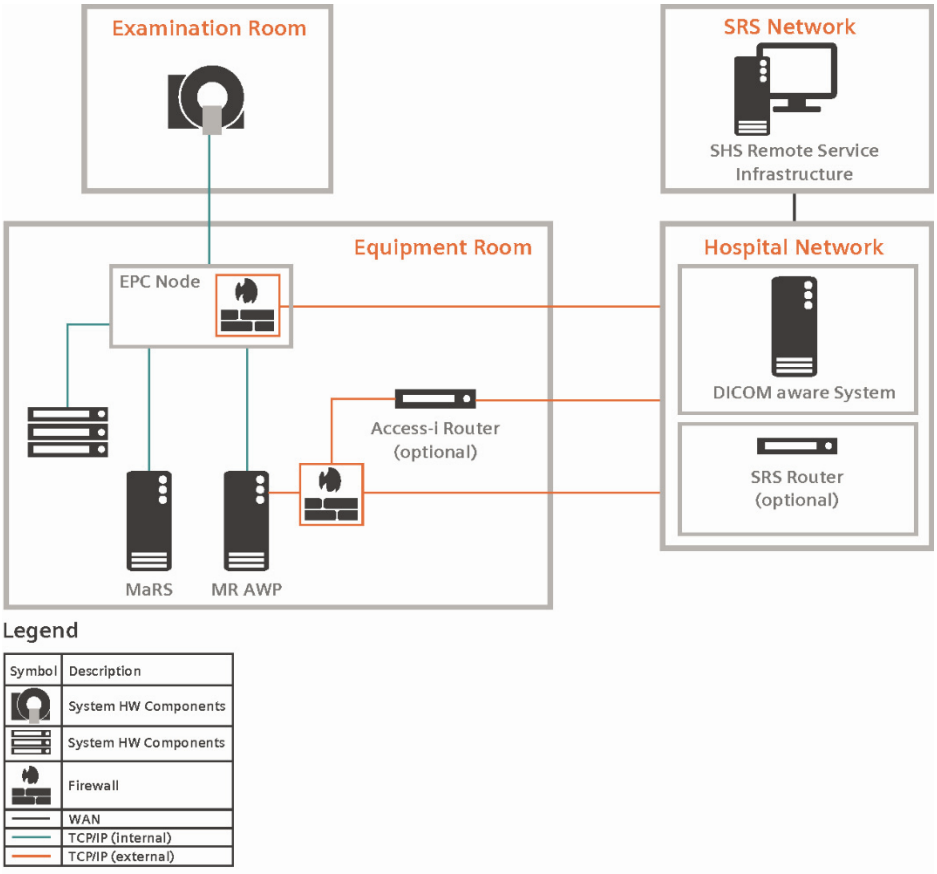
Boundary defense
- Built-in firewall is used to minimize the network attack surface.
- For optimized protection of sensitive data and operation of the system it must be deployed in a secure network environment, utilizing e.g. network segmentation, client access control and protection against access from public networks.
- Security best practices suggest that boundary defenses in the hospital should be multilayered relying on firewalls, proxies, demilitarized zone (DMZ) and network-based intrusion detection systems (IDS) and instrusion prevention systems (IPS), as well as physical protections

Attack boundaries
For your risk control, consider the following attack mechanisms that a malicious or negligent user could potentially use:
- via the user interface, for example, calling up a recently measured patient and reading its PHI
- via USB flash drives, for example, copying information from the system to a USB flash drive
- via network, for example, exploiting newly detected vulnerabilities to attack the system.

Information below may help you in mitigating security hazards arising from these attack mechanisms.

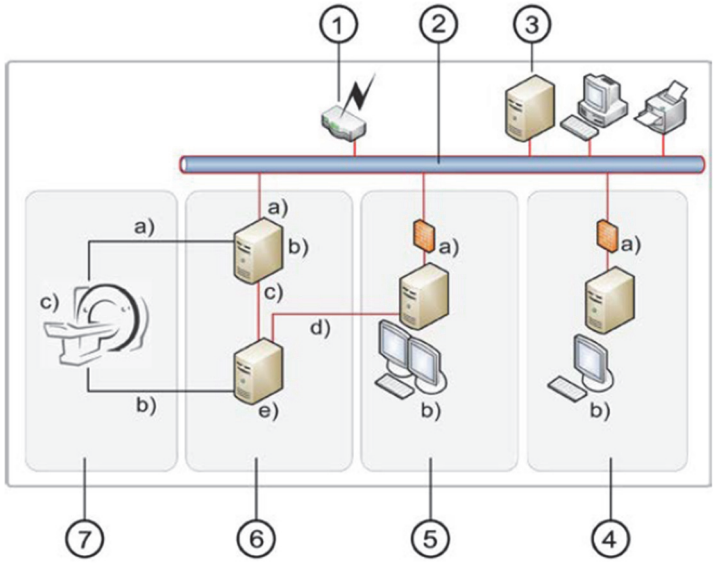
Network information

MAGNETOM Free.Max, Free.Star



Access-i Router	Siemens Healthineers Access-i router (optional)
MR AWP	*syngo* Acquisition Workplace
MaRS	Measurement and Reconstruction System
DICOM aware systems	Systems such as RIS, PACS, printer, postprocessing workstation
SRS Router	Smart Remote Service router

MAGNETOM Vida, Lumina, Vida Fit, Skyra Fit, Avanto Fit



(1) Siemens Healthineers Remote Service router

(2) Hospital network

(3) DICOM nodes such as RIS, PACS, printer, postprocessing WS

(4) Hospital room

a) Firewall

b) *syngo* MR Workplace (optional)

(5) Operator room

a) Firewall

b) *syngo* Acquisition Workplace

(6) Equipment room

a) HTTPS only

b) CAN24 unit

c) TCP/IP (internal)

d) TCP/IP (internal)

e) Measurement and reconstruction system (MARS)

(7) Examination room

a) CAN bus

b) Fibreoptics cable

c) MRI

The basic MR system is situated in three separate but adjacent rooms: The examination room where the patient is examined, the operator room where the medical operators work, and the equipment room where most of the control hardware is installed.

Communication lines shown in red are Ethernet connections (TCP and UDP). Communication lines shown in black use other internal protocols (CAN, PCIe, or proprietary protocols). The internal Ethernet connections between the *syngo* Acquisition Workplace and the MARS and between the CAN24 and the MARS are not accessible from the hospital network.

It is assumed that the equipment room is locked and not accessible to patients or non-authorized personnel. If the room is left open for mitigation of fire hazards, at least an intrusion alarm should be present. For installations with elevated security requirements, it is recommended to make the operator room inaccessible to patients and non-authorized persons.

Optional components:

- The *syngo* MR Workplace is an optional workstation for image viewing and postprocessing. It could even be situated in a separate room. Information in the patient and image database located on the *syngo* Acquisition Workplace is shared between the *syngo* Acquisition Workplace and the *syngo* MR Workplace, i.e. sensitive information is transferred over the hospital network. For systems with elevated security requirements, it is recommended to either not use the *syngo* MR Workplace or to make sure that the network communication between the *syngo* Acquisition Workplace and the *syngo* MR Workplace is secured.
- Siemens Remote Service is an optional feature. Without remote service, the router to the Siemens service center is not needed.
- The CAN24 unit is used to monitor the magnet status by remote service even if the other system parts are switched off. Without remote service, this cannot be done. The CAN24 is not optional; however, the connection to the hospital network can be omitted.

The *syngo* MR Workplace requires one static IP address, which must be provided by the customer.

Port number	Service/function	Direction (in/out)	Protcol
MR AWP			
80	Web Server HTTP	in	TCP
104	DICOM Server	in	TCP
443	Secure Web Server HTTPS	in	TCP
2000	MR Exam	in	TCP
2762	DICOM Server	in	TCP
3389	Microsoft Terminal Services	in	TCP
5905	MR Expert-i Licensing	in	TCP
7443	syngo.WebExpert-i	in	TCP
7788	MR Exam	in	TCP
8090	OnlineHelp Repository	in	TCP
32912	syngo client/server communication services	in	TCP
32914	syngo communication services	in	TCP
67	MR DHCP	in	UDP
123	MR Time Server	in	UDP
7787	Access-i HTTPS (optional)	in	TCP
7788	Access-i Websocket (optional)	in	TCP
7789	Access-i Elastrography (optional)	in	TCP

Table 1: Firewall external open ports

Additional dynamic ports might result to be open during operation of the system.

Security controls

Malware Protection
syngo MR XA50 prevents the installation and infection from malwares by means of:

- Whitelisting (Microsoft® Device Guard)

Controlled Use of Administrative Privileges
- The system distinguishes between clinical and administrative roles. Clinical users do not require administrative privileges. Authorization as administrator is required for administrative tasks.

Authentication
- *syngo* MR XA50 supports HIPAA (Health Insurance Portability and Accountability Act) regulation with role-based privilege assignment and access control.
- The user interface of *syngo* MR XA50 provides a screen lock functionality that can be engaged manually or automatically after a certain time of inactivity. For details refer to the system owner manual.

Security Scanning
Basic security scans are run by many medical device customers on their network. This device was scanned during development utilizing the Nessus scanning tool. Siemens Healthineers cannot test this device against every scanner on the market. In addition Siemens Healthineers is unable to confirm that scanning this device will not produce harmful effects on the device that may render the device out of service temporarily or permanently. To ensure patient safety, scanning of this device is not allowed during clinical use. It is strongly recommended to perform uncredentialed scans only and to reboot the system after the scan is finished.

Continuous Vulnerability Monitoring
Continuous vulnerability assessment and remediation is performed.

Hardening
syngo MR XA50 hardening is performed based on the Security Technical Implementation Guidelines (STIG's) developed by the Defense Information Systems Agency (DISA).

Network Controls
The system is designed to make limited use of network ports and protocols. Only ports and protocols which are required for operation are open and utilized.Windows Defender Firewall is configured to block unwanted inbound network traffic except for those mentioned in

- **Table 1: Firewall external open ports**.
- Siemens Healthineers recommends operating the system in a secured network environment, e.g. a separate network segment or a Virtual Local Area Network (VLAN).
- Connection to the internet or private networks for patients/guests is not recommended.
- In case of a denial of service (DoS) attack, the system can be taken off the network and operated standalone.

Physical Safeguards
The customer is responsible for the physical protection of the MAGNETOM system and the operating consoles, for example, by securing the operator and equipment room with user access control and by following the suggested controls (system dependent):
- Restricting access to the operator room so that no unauthorized person can enter it easily.
- Placing the *syngo* Acquisition Workplace PC in a closed cabinet so that it cannot be removed easily.
- Chaining the computers to a wall, using a chain or a steel cable and a padlock.
- Preventing unauthorized persons from accessing the network, for example, by securing network connectors and making unused network ports inaccessible.
- Or a combination of these measures, for additional security.

Data Protection Controls

- The system is not intended to be used as an archive (data at rest).
- PHI is protected by role-based access control.
- The system provides auditing of PHI access control.
- For confidentiality and integrity of PHI/PII data during transport, the PHI/PII data can be encrypted. Note: encrypted communication can be used if all connected DICOM nodes support encrypted communication. The MR system is connected to the hospital network via Ethernet. Image transfer to the archive system and postprocessing nodes is performed using the DICOM protocol.
- For protection of PHI data in transit, DICOM encryption is supported.

Auditing/Logging

Audit information is stored locally and access is limited by means of the operating system to administrative users. Additionally the audited information can be sent to a server by applying the Syslog protocol. Encryption via secure TCP is optional.
The audit trail contains the following information:
• Access, modification, creation and deletion of PHI
• Login and logout activity of users
• Access to privileged functions

Remote Connectivity

syngo MR XA50 system can be connected to Smart Remote Services (SRS). Connection to SRS is performed via an encrypted VPN channel only.
For more information about remote connection, an SRS Security White Paper is available from your local Siemens Healthineers organization.

Incident Response and Management

An incident handling process is defined and being executed on demand to handle cybersecurity incidents with high priority.

Shared responsibilities

The customer is responsible for physically securing the *syngo* MR XA50 in a secure location, for proper access management and proper network security for the network to which the *syngo* MR XA50 system is connected and over which it transfers data.

Software bill of materials[1]

The following table lists the most relevant third-party technologies used. A complete list of software components is available on tpFleet or directly from the producer.

Vendor name	Component name	Component version	Description/use
Microsoft	Windows 10	IoT Enterprise LTSC 1909 64-Bit	Operating System
Microsoft	SQL Server	2016	Database
Microsoft	.NET Framework	4.8	Program runtime environment
Adobe	Adobe Reader DC	2020.006.20042	Report viewer / Offline documentation
TechSmith	Camtasia	1.1.1	Screen capture
Ultra VNC	Ultra VNC	1.2.1.0	Otional: Expert-I VNC Viewer
Display Link	Display Link Graphics Driver	8.6 M1	Support for Patient Data Display

[1] *For supported countries. Requires a customer account in teamplay Fleet. Please contact your local Siemens Healthineers organization for further details.*

Manufacturer Disclosure Statement (MDS²)

Question ID	Question	Answer	See Note
DOC-1	Manufacturer Name	Siemens Healthcare GmbH	
DOC-2	Device Description	The MAGNETOM systems are magnetic resonance imaging (MRI) devices that produce transverse, sagittal, coronal and oblique cross-sectional images, spectroscopic images and/or spectra, and display the internal structure and/or function of the head, body, or extremities. To generate clinically relevant images MRI systems include the following main components/subsystems: - a magnet with a main magnetic field, - a gradient system, - the radio-frequency system and - a computer system incl. dedicated software	
DOC-3	Device Model	MAGNETOM Systems	
DOC-4	Document ID	Print No. M11-03002G.629.08.01.i02	
DOC-5	Manufacturer Contact Information	https://www.siemens-healthineers.com/magnetic-resonance-imaging	
DOC-6	Intended use of device in network-connected environment:	The MRI Scanner is used to create diagnostic images which can be sent via the local network to DICOM nodes. Note: External network connection (e.g. hospital network) is not mandatory to operate MAGNETOM systems.	
DOC-7	Document Release Date	2021-11-30	

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 section Network Information	
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 (MPII)

Question ID	Question	Answer	Note
MPII-1	Can this device display, transmit, store, or modify personally identifiable information (e.g. electronic Protected Health Information (ePHI))?	Yes. MR Scanner are producing, storing, displaying, transmitting and receiving PHI, identified (name or IDs ...) and identifiable (DICOM Images, timestamps, location ...) attributes.	
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, only for a short time of period.	
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?	Yes	
MPII-2.5	Does the device allow configuration to automatically delete local personally identifiable	Yes	

MPII-2.5	information after it is stored to a long term solution?		
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. DICOM send, Export to a server, USB device ...; Sending Data to an audit trail server (SysLog)	
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)?	Yes	
MPII-2.9	Does the device allow personally identifiable information records be stored in a separate location from the device's operating system (i.e. secondary internal drive, alternate drive partition, or remote storage location)?	No	
MPII-3	Does the device have mechanisms used for the transmitting, importing/exporting of personally identifiable information?	Yes	
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?	No. Printers/cameras can be connected on customer side to generate hard copies.	
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, via USB.	
MPII-3.5	Does the device transmit/receive personally identifiable information via a wired network connection (e.g., RJ45, fiber optic, etc.)?	Yes	
MPII-3.6	Does the device transmit/receive personally identifiable information via a wireless network connection (e.g., WiFi, Bluetooth, NFC, infrared, cellular, etc.)?	No	
MPII-3.7	Does the device transmit/receive personally identifiable information over an external network (e.g., Internet)?	Yes	
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?	Yes. Other means are Access-I (if it is supported), Virtual Cockpit and Expert-I.	

Management of Private Data notes:

Automatic logoff (ALOF)

The device's ability to prevent access and misuse by unauthorized users if device is left idle for a period of time.

Question ID	Question	Answer	Note
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)?	Yes, session lock	
ALOF-2	Is the length of inactivity time before auto-logoff/screen lock user or administrator configurable?	Yes	

Audit controls (AUDT)

The ability to reliably audit activity on the device.

Question ID	Question	Answer	Note
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. User information and Patient ID nearly for every audit trail log entry.	
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)?	Yes	
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?	Yes	
AUDT-2.8.2	Application Programming Interface (API) and similar activity?	Yes. Access to PHI/PII is logged	
AUDT-2.9	Emergency access?	Yes. Emergency user operation is logged.	
AUDT-2.10	Other events (e.g., software updates)?	Yes	
AUDT-2.11	Is the audit capability documented in more detail?	Yes, in the Operator Manual – MR System Administration	
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?	Yes	
AUDT-5.2	Via IHE Audit Trail and Node Authentication (ATNA) profile to SIEM?	Yes. The audit trail can be written to externa SYSLOG server	
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. Encrypted syslog server is supported. Local audit logs files can only be read by an administrator.	
AUDT-6	Can audit logs be monitored/reviewed by owner/operator?	Yes. Only authorized users are allowed to inspect audit trail records.	
AUDT-7	Are audit logs protected from modification?	Yes	

AUDT-7.1	Are audit logs protected from access?	Yes, accessible for administrator only	
AUDT-8	Can audit logs be analyzed by the device?	Yes. If the audit trails are stored on the local file system, evaluation of the audit trail logs can be done in the OS Save Log Viewer	

Authorization (AUTH)

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

Question ID	Question	Answer	Note
AUTH-1	Does the device prevent access to unauthorized users through user login requirements or other mechanism?	Yes	
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	
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)?	Yes	
AUTH-4	Does the device authorize or control all API access requests?	No	
AUTH-5	Does the device run in a restricted access mode, or 'kiosk mode', by default?	Yes	

Cybersecurity product upgrades (CSUP)

The ability of on-site service staff, remote service staff, or authorized customer staff to install/upgrade device's security patches.

Question ID	Question	Answer	Note
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	Yes	

CSUP-1	of the software/firmware? If no, answer “N/A” to questions in this section.		
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?	No	
CSUP-2.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	No, only the medical device manufacturer is allowed to install patches or software updates	
CSUP-2.3	Does the device have the capability to receive remote installation of patches or software updates?	Yes, for selected patch/update types	
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?	No	
CSUP-3.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	Yes, only the medical device manufacturer is allowed to install patches or software updates	
CSUP-3.3	Does the device have the capability to receive remote installation of patches or software updates?	Yes	
CSUP-3.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	No	
CSUP-4	Does the device contain Anti-Malware Software? If yes, complete 4.1-4.4.	Yes	
CSUP-4.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	No	
CSUP-4.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	No, only the medical device manufacturer is allowed to install patches or software updates	
CSUP-4.3	Does the device have the capability to receive remote installation of patches or software updates?	Yes, for selected patch/update types	
CSUP-4.4	Does the medical device manufacturer allow security updates from any third-party	N/A, not needed for whitelisting	

CSUP-4.4	manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?		
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?	No	
CSUP-5.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	No, only the medical device manufacturer is allowed to install patches or software updates	
CSUP-5.3	Does the device have the capability to receive remote installation of patches or software updates?	Yes, for selected patch/update types	
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.	Yes	
CSUP-6.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	No	
CSUP-6.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	No, only the medical device manufacturer is allowed to install patches or software updates	
CSUP-6.3	Does the device have the capability to receive remote installation of patches or software updates?	Yes, for selected patch/update types	
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?	No	
CSUP-7	Does the manufacturer notify the customer when updates are approved for installation?	Yes, if the device is under service contract	
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?	No	
CSUP-10	Can the owner/operator install manufacturer-approved third-party software on the device themselves?	Yes, for specific services only, i.e., OpenApps.	

CSUP-10.1	Does the system have mechanism in place to prevent installation of unapproved software?	Yes	
CSUP-11	Does the manufacturer have a process in place to assess device vulnerabilities and updates?	Yes	
CSUP-11.1	Does the manufacturer provide customers with review and approval status of updates?	Yes, in teamplay Fleet	
CSUP-11.2	Is there an update review cycle for the device?	Yes, updates are provided in regular cycles	

Health data de-identification (DIDT)

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

Question ID	Question	Answer	Note
DIDT-1	Does the device provide an integral capability to de-identify personally identifiable information?	No, only data minimization is supported, data is not de-identified complete and still contains information like patient names.	
DIDT-1.1	Does the device support de-identification profiles that comply with the DICOM standard for de-identification?	Yes. MR provides three levels of so called anonymization. Patients names are still included in Structured report or DICOM SC RGB.	

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	Note
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?	Yes, Service data and configuration data can be backed up on an external drive by the service technician.	
DTBK-4	Does the device have an integral data backup capability to remote storage?	No. MR provides the capability to transfer data to external customer storage if any. This is also strongly recommended.	

DTBK-5	Does the device have a backup capability for system configuration information, patch restoration, and software restoration?	Yes, for system configuration information	
DTBK-6	Does the device provide the capability to check the integrity and authenticity of a backup?	No	

Emergency access (EMRG)

The ability of the device user to access personally identifiable information in case of a medical emergency situation that requires immediate access to stored personally identifiable information.

Question ID	Question	Answer	Note
EMRG-1	Does the device incorporate an emergency access (i.e. “break-glass”) feature?	No	

Health data integrity and authenticity (IGAU)

How the device ensures that the stored data on the device has not been altered or destroyed in a non-authorized manner and is from the originator.

Question ID	Question	Answer	Note
IGAU-1	Does the device provide data integrity checking mechanisms of stored health data (e.g., hash or digital signature)?	No, the medical device is not intended to be used for patient data storage. Patient data should be transferred immediately to an appropriate archive.	
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	Note
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.	Yes. Device Guard is used.	
MLDP-2.1	Does the device include anti-malware software by default?	Yes	

MLDP-2.2	Does the device have anti-malware software available as an option?	N/A	
MLDP-2.3	Does the device documentation allow the owner/operator to install or update anti-malware software?	No. MR anti-malware solution is fully managed.	
MLDP-2.4	Can the device owner/operator independently (re-)configure anti-malware settings?	No	
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?	N/A	
MLDP-2.8	Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)?	Yes, the protection of the system is based on Whitelisting and therefore no additional Anti Virus Software is needed.	
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?	N/A	
MLDP-4	Does the device employ application whitelisting that restricts the software and services that are permitted to be run on the device?	Yes, Microsoft® Device Guard is used to protect the system.	
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	Note
NAUT-1	Does the device provide/support any means of node authentication that assures both the sender and the recipient of data are known to each other and are authorized to receive transferred information (e.g. Web APIs, SMTP, SNMP)?	No, for remote service access (e.g. Siemens Remote Service) technical measures for node authentication are in place.	
NAUT-2	Are network access control mechanisms supported (E.g., does the device have an internal firewall, or use a network connection white list)?	Yes, internal firewall is available	

NAUT-2.1	Is the firewall ruleset documented and available for review?	Yes, see Security Whitepaper	
NAUT-3	Does the device use certificate-based network connection authentication?	Yes, e.g., DICOM trusted nodes, Expert-I, Access-I	

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	Note
CONN-1	Does the device have hardware connectivity capabilities?	Yes	
CONN-1.1	Does the device support wireless connections?	No	
CONN-1.1.1	Does the device support Wi-Fi?	No, MR scanner do not support Wi-Fi.	
CONN-1.1.2	Does the device support Bluetooth?	No	
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)?	Yes. PMU (physiological Measurement Unit)	
CONN-1.2	Does the device support physical connections?	Yes	
CONN-1.2.1	Does the device have available RJ45 Ethernet ports?	Yes	
CONN-1.2.2	Does the device have available USB ports?	Yes	
CONN-1.2.3	Does the device require, use, or support removable memory devices?	Yes	
CONN-1.2.4	Does the device support other physical connectivity?	Yes. Graphics ports, Serial Port.	
CONN-2	Does the manufacturer provide a list of network ports and protocols that are used or may be used on the device?	Yes, see Security Whitepaper	
CONN-3	Can the device communicate with other systems within the customer environment?	Yes, e.g. PACS, Printer and other medical devices (DICOM)	
CONN-4	Can the device communicate with other systems external to the customer environment (e.g., a service host)?	Yes, e.g., SRS, Access-i.	

CONN-5	Does the device make or receive API calls?	Yes	
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	
CONN-7.1	Is TLS configurable?	No, not by the customer	
CONN-8	Does the device provide operator control functionality from a separate device (e.g., telemedicine)?	Yes. Access-i, Expert-i, *syngo* Virtual Cockpit (SVC)	

Person authentication (PAUT)

The ability to configure the device to authenticate users.

Question ID	Question	Answer	Note
PAUT-1	Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)?	No, but customer defined user accounts possible	
PAUT-1.1	Does the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)?	No, but customer defined user accounts possible	
PAUT-2	Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, etc.)?	No	
PAUT-3	Is the device configurable to lock out a user after a certain number of unsuccessful logon attempts?	No	
PAUT-4	Are all default accounts (e.g., technician service accounts, administrator accounts) listed in the documentation?	Yes	
PAUT-5	Can all passwords be changed?	Yes	
PAUT-6	Is the device configurable to enforce creation of user account passwords that meet established (organization specific) complexity rules?	Yes	
PAUT-7	Does the device support account passwords that expire periodically?	Yes, configurable	
PAUT-8	Does the device support multi-factor authentication?	No	
PAUT-9	Does the device support single sign-on (SSO)?	No	
PAUT-10	Can user accounts be disabled/locked on the device?	Yes	

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, as provided by Windows 10	
PAUT-14.1	Are credentials stored using a secure method?	Yes, as provided by Windows 10	

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	Note
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, customer can physically secure the device with very little effort.	
PLOK-3	Are all device components maintaining personally identifiable information (other than removable media) physically secured behind an individually keyed locking device?	No, customer can physically secure the device with very little effort.	
PLOK-4	Does the device have an option for the customer to attach a physical lock to restrict access to removable media?	No, customer can physically secure the device with very little effort.	

Roadmap for third party applications and software components in device life cycle (RDMP)

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

Question ID	Question	Answer	Note
RDMP-1	Was a secure software development process, such as ISO/IEC 27034 or IEC 62304, followed during product development?	Yes	
RDMP-2	Does the manufacturer evaluate third-party applications and software components included in the device for secure development practices?	Yes, according to IEC 62304	

RDMP-3	Does the manufacturer maintain a web page or other source of information on software support dates and updates?	Yes, this information is managed internally.	
RDMP-4	Does the manufacturer have a plan for managing third-party component end-of-life?	Yes	

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	Note
SBOM-1	Is the SBoM for this product available?	Yes, refer to the Security Whitepaper.	
SBOM-2	Does the SBoM follow a standard or common method in describing software components?	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?	Yes	
SBOM-3	Does the device include a command or process method available to generate a list of software components installed on the device?	Yes	
SBOM-4	Is there an update process for the SBoM?	Yes	

System and application hardening (SAHD)

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

Question ID	Question	Answer	Note
SAHD-1	Is the device hardened in accordance with any industry standards?	Yes, following DISA Stigs	
SAHD-2	Has the device received any cybersecurity certifications?	No	
SAHD-3	Does the device employ any mechanisms for software integrity checking	Yes	

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	
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	
SAHD-4	Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)?	No, done automatically by the system	
SAHD-5	Is the system configurable to allow the implementation of file-level, patient level, or other types of access controls?	Yes	
SAHD-5.1	Does the device provide role-based access controls?	Yes	
SAHD-6	Are any system or user accounts Unrestricted or disabled by the manufacturer at system delivery?	No	
SAHD-6.1	Are any system or user accounts configurable by the end user after initial configuration?	Yes, by the administrator	
SAHD-6.2	Does this include restricting certain system or user accounts, such as service technicians, to least privileged access?	Yes	
SAHD-7	Are all shared resources (e.g., file shares) which are not required for the intended use of the device disabled?	Yes	
SAHD-8	Are all communication ports and protocols that are not required for the intended use of the device disabled?	Yes	
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	
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	
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, can be disabled on request	
SAHD-12	Can unauthorized software or hardware be installed on the device without the use of physical tools?	No	
SAHD-13	Does the product documentation include information on operational network security scanning by users?	No	

SAHD-14	Can the device be hardened beyond the default provided state?	Yes, only by the manufacturer	
SAHD-14.1	Are instructions available from vendor for increased hardening?	Yes	
SHAD-15	Can the system prevent access to BIOS or other bootloaders during boot?	Yes	
SAHD-16	Have additional hardening methods not included in 2.3.19 been used to harden the device?	No, but additional security measures are in place	

Security guidance (SGUD)

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

Question ID	Question	Answer	Note
SGUD-1	Does the device include security documentation for the owner/operator?	Yes	
SGUD-2	Does the device have the capability, and provide instructions, for the permanent deletion of data from the device or media?	Yes, Siemens Service has instructions in place to support the customer during the device/media sanitization.	
SGUD-3	Are all access accounts documented?	Yes	
SGUD-3.1	Can the owner/operator manage password control for all accounts?	No, for customer user accounts only	
SGUD-4	Does the product include documentation on recommended compensating controls for the device?	Yes	

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	Note
STCF-1	Can the device encrypt data at rest?	No	
STCF-1.1	Is all data encrypted or otherwise protected?	No	
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?	Yes, by the manufacturer	

STCF-3	Is the data stored in a database located on the device?	Yes	
STCF-4	Is the data stored in a database external to the device?	Yes, customer responsibility (e.g., PACS)	

Transmission confidentiality (TXCF)

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

Question ID	Question	Answer	Note
TXCF-1	Can personally identifiable information be transmitted only via a point-to-point dedicated cable?	No, depends on the customer network design. In principle possible but not common.	
TXCF-2	Is personally identifiable information encrypted prior to transmission via a network or removable media?	No, DICOM Encryption is supported and can be configured. Software based removable media encryption is not supported.	
TXCF-2.1	If data is not encrypted by default, can the customer configure encryption options?	Yes	
TXCF-3	Is personally identifiable information transmission Unrestricted to a fixed list of network destinations?	Yes, DICOM nodes are defined and identified using their IP address	
TXCF-4	Are connections limited to authenticated systems?	No, but DICOM trusted nodes can be configured.	
TXCF-5	Are secure transmission methods supported/implemented (DICOM, HL7, IEEE 11073)?	Yes, DICOM Encryption	

Transmission integrity (TXIG)

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

Question ID	Question	Answer	Note
TXIG-1	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission?	No. Verification option are available.	
TXIG-2	Does the device include multiple sub-components connected by external cables?	No	

Remote service (RMOT)

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

Question ID	Question	Answer	Note
RMOT-1	Does the device permit remote service connections for device analysis or repair?	Yes	
RMOT-1.1	Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair?	Yes	
RMOT-1.2	Is there an indicator for an enabled and active remote session?	Yes	
RMOT-1.3	Can patient data be accessed or viewed from the device during the remote session?	Yes	
RMOT-2	Does the device permit or use remote service connections for predictive maintenance data?	Yes	
RMOT-3	Does the device have any other remotely accessible functionality (e.g. software updates, remote training)?	Yes	

Other security considerations (OTHR)

NONE

Notes

n.a.	n.a.

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 Service**s**
HIPAA	Health Insurance Portability and Accountability Act
HIMSS	Healthcare Information and Management Systems Society
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
IEC	International Electrotechnical Commission
LDAP	Lightweight Directory Access Protocol
MD5	RSA Data Security, Inc. MD5 Message-Digest Algorithm
MDS²	Manufacturer Disclosure Statement for Medical Device Security
NEMA	National Electrical Manufacturers Association
NTP	Network Time Protocol
OCR	Office for Civil Rights
PHI	Protected Health Information
PII	Personally Identifiable Information
RPC	Remote Procedure Call
SHA	Secure Hash Algorithm
SQL	Structured Query Language
SRS	Smart Remote Services
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 Healthcare - voids all warranties, liabilities, assertions and contracts.

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

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

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

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

Statement on FDA Cybersecurity Guidance

Siemens Healthineers will follow cybersecurity guidance issued by the FDA as appropriate. Siemens Healthineers recognizes the principle described in FDA cybersecurity guidance that an effective cybersecurity framework is a shared responsibility among multiple stakeholders (e.g., medical device manufacturers, health care 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 whitepaper 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.

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 no-tice. 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