White paper

MAMMOMAT B.brilliant VA10 Security white paper and MDS[2]

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 lifecycle of our products.

Our program aims to incorporate 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 resilience of our products to 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 regarding reported potential vulnerabilities. Our communications policy strives for coordinated disclosure. We work in this way with our customers and other parties, where 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 analyses for our products
- Incorporating security-focused 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 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 be reported by email to:

productsecurity@siemens-healthineers.com

Jim Jacobson
Chief Product and Solution Security Officer
Siemens Healthineers

Contents

Basic information

Every day, physicians and nurses provide guidance, reassurance, and expertise to women across the globe. In the fight against breast cancer, we do what we can to offer support. We believe that our biggest impact lies in complementing your experience with ours – our track record of technological breakthroughs. When it comes to breast cancer screening and diagnosis, we strive to provide you and your patients with the most accurate diagnostic results.

With MAMMOMAT B.brilliant, we are breaking new ground. It aims to offer uncompromised cancer detection for women who want straightforward answers. Experience higher accuracy[1], easy workflows[1], and efficient diagnostic processes – in a next-generation mammography system that was developed with women's wellbeing in mind.

MAMMOMAT B.brilliant is the first mammography device featuring PlatinumTomo combining 50° Wide-Angle Tomosynthesis and impressive acquisition speed with excellent in-plane resolution and customizable image impression. At the same time, MAMMOMAT B.brilliant is easy to work with – offering convenient decision processes for all mammography-based diagnostic applications.[1]

Inventory of devices

The main operator console of the MAMMOMAT B.brilliant is a Windows 10 based PC with the proprietary X-ray acquisition software (AWS) based on *syngo*. The AWS PC is externally connected via DICOM connection to the hospital network in order to send and receive clinical data (images, RIS worklist, reports, ...). This is a wired network connection.

Internally the AWS PC is connected to the X-ray generator and mechanical system via a proprietary protocol based on optical Ethernet. Additionally the AWS PC is internally connected to an X-ray detector via a proprietary protocol based on optical Ethernet. For details see Figure 1.

Operating system

Microsoft Windows 10 Enterprise LTSC 2019 (64 bit)

Hardware specifications

The main operator console of the MAMMOMAT B.brilliant is hosted on a Windows 10 based PC with 3 network interfaces (see Figure 1).

User account information

MAMMOMAT B.brilliant supports the HIPAA (Health Insurance Portability and Accountability Act) regulation with role-based privilege assignment and access control.

MAMMOMAT B.brilliant provides the possibility to use an existing Active Directory infrastructure for user authentication and authorization.

Patching strategy

Security patches will be provided on a regular basis, after internal validation by Siemens Healthineers.

Cryptography usage

The following cryptographic algorithms are applied by MAMMOMAT B.brilliant:

- TLS 1.2 is used for:
  - Secure DICOM
  - HTTPS connection for Smart Remote Services
- SHA-256 is used for digital signature of the binaries in the context of whitelisting

All cryptography algorithms applied by MAMMOMAT B.brilliant for TLS 1.2 are FIPS 140-2 compliant.

[1] *Data on file*

Basic information

Handling of sensitive data

The MAMMOMAT B.brilliant system is designed for temporary data storage only. Siemens Healthineers recommends storing relevant data to a long-term archive, e.g., on a PACS, and to subsequently delete the data on the scanner automatically or manually.

Protected Health Information (PHI) is temporarily stored on the MAMMOMAT B.brilliant system (DICOM data, raw data, meta data for DICOM creation). The storage duration for PHI can be influenced by the customer.

Personally Identifiable Information (PII) as part of the DICOM records is also temporarily stored on the MAMMOMAT B.brilliant system, e.g., patient's name, birthday or age, height and weight, personal identification number, referring physician's name. Additional sensitive information might be present in user editable input fields or in the images acquired.

PHI data is stored into Audit Trail according to HIPAA.

Protected Health Information (PHI) is transmitted via DICOM (encrypted/unencrypted).

Data recovery

It is assumed that Personal Health Information (PHI) is archived to a PACS after patient examination is completed or images are ready after post processing.

The system supports backup and restore of system configuration to an external drive.

Boundary defense

A 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

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

Network information

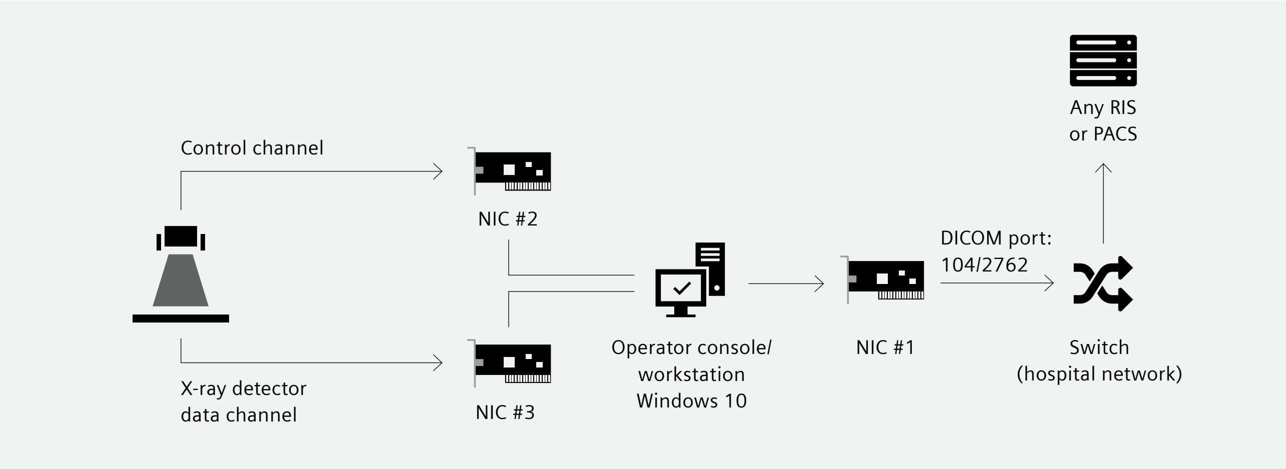

Figure 1: Network connections

Network information

In order to be fully operable, MAMMOMAT B.brilliant requires the following ports to be opened toward the clinical network.

Port number	Service/function	Direction (in/out)	Protocol
53	DNS	out	UDP, TCP
67	DHCP	out	UDP
88	Kerberos	out	UDP, TCP
123	NTP	out	UDP
80, 443	Remote Web Service	in	TCP
Configurable by customer	Central Syslog	out	UDP, TCP
104, 2762	DICOM	in	TCP
Configurable by customer	DICOM	out	TCP
389	Active Directory	out	TCP
8226, 13001	Managed Node Package (MNP)	in	TCP
8227, 8228, 12061	Managed Node Package (MNP)	out	TCP
11080, 11081	Remote Assist – Team Viewer	in	TCP
8080	Knowledge Base	out	TCP
20, 21	FTP	in, out	TCP

Allowed services accessible through network running on the device:

Service	Description	Startup type	Log on as
RCA MSI Redirector	Radia Client Automation MSI Redirector	Automatic*	Local system
RCA Notify Daemon	Radia Client Automation Notify Daemon	Automatic*	Local system
RCA Scheduler Daemon	Radia Client Automation Scheduler Daemon	Automatic*	Local system
syngo.Services.FileTransferService	Hosts the FileTransfer services	Automatic	Local system
World Wide Web Publishing Service	Provides Web connectivity and administration through the Internet Information Services Manager	Automatic	Local system

**If System Management is not configured these services are disabled.*

Security controls

Malware protection

- Whitelisting is realized by Microsoft Device Guard.
- Additional protection is given by applying Microsoft AppLocker.

Controlled use of administrative privileges

The system distinguishes between clinical and administrative roles (optional). Clinical users do not require administrative privileges. Authorization as administrator is required for administrative tasks.

Authentication

MAMMOMAT B.brilliant supports the HIPAA (Health Insurance Portability and Accountability Act) regulation with role-based privilege assignment and access control (optional).

MAMMOMAT B.brilliant supports authentication of local users as well as authentication of users defined in an active directory (optional).

The MAMMOMAT B.brilliant user interface provides a screen lock function that can be engaged manually or automatically after a certain inactivity time (optional).

Security scanning

Basic security scans are run by many customers on medical devices on their network. Although this device was scanned during development using the Tenable Nessus scanning tool, Siemens Healthineers cannot test this device against every scanner on the market and 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. Scanning of this device is not allowed during clinical use. It is strongly recommended that users only perform uncredentialed scans and reboot the system after the scan is finished.

Continuous vulnerability monitoring

Siemens Healthineers performs vulnerability monitoring of the included third-party components (including the operating system). Vulnerabilities are assessed regarding their criticality and safety relevance. In case of critical vulnerabilities the associated hotfixes are distributed within a system service pack. Service packs can be installed via Smart Remote Services, by customer via download from teamplay Fleet or by a Siemens Healthineers service technician – depending on the availability of the Smart Remote Services infrastructure at the customer’s site and on the impact of the service pack.

Hardening

Hardening of the file system and of proprietary software was performed according to the principle of least privilege.

The network attack surface was restricted by only allowing network communication which is essential for operating the MAMMOMAT B.brilliant device.

Hardening of third-party software is performed according to the Security Technical Implementation Guidelines developed by the Defense Information Systems Agency (DISA).

Furthermore the customer has the possibility to disable the connection of USB mass storage devices.

Network controls

Windows Firewall is configured to block unwanted inbound network traffic, except for the above-mentioned ports.

Siemens Healthineers recommends operating the system in a secured network environment, e.g., a separate network segment or a VLAN.

Connecting MAMMOMAT B.brilliant system to the internet or to private networks for patients/guests is not recommended.

Security controls

Physical safeguards
The AWS PC is mounted in a case in the control table (available as an option).

The Customer is responsible for the physical protection of the AWS PC.

Data protection controls
Personal Health Information (PHI) is protected by role-based access control (optional).

MAMMOMAT B.brilliant provides auditing of PHI access (optional). Audit logs are access-controlled.

Confidentiality and integrity of PHI/PII data can be protected by encryption of DICOM communication with other DICOM nodes.

Auditing/Logging
MAMMOMAT B.brilliant supports HIPAA-compliant auditing of operations on PHI, PII and user information (i.e., login, read access PHI, modification of PHI) (optional).

Audit logs stored locally are access-controlled and access is provided to authorized personnel only. The administrator has the possibility to export the audit logs to the configured device.

Audit entries contain user name, action performed, result of the action, Hostname, IP Address, MAC address, Hospital Name, Location, Version Of Software, Serial Number, Site Identification Number, HIS/RIS Application Entity Title, DICOM Node Application Entity Title, DICOM Printer Application Entity Title, Time and Time Zone.

Remote connectivity
The MAMMOMAT B.brilliant system can be connected to Smart Remote Services (SRS). Connection to SRS is performed via an encrypted VPN channel only. A Security white paper for SRS is available from your local Siemens Healthineers organization.

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

Shared responsibilities

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

Software bill of materials

The following list comprises the most relevant third-party technologies used.
A comprehensive list can be provided on request.

- Microsoft Windows 10 Enterprise LTSC 2019 (64 bit)
- Adobe Acrobat Reader
- Merge DICOM Toolkit
- Actian NoSQL Database
- Nvidia Graphic Card Driver
- Nvidia CUDA Toolkit
- Accelerite Radia Endpoint Manager
- Micro Focus Operations Agent
- Teamviewer
- Microsoft .NET Framework
- Microsoft Visual C++ Redistributables
- Intel Integrated Performance Primitives

Manufacturer Disclosure Statement (MDS²)

Question ID	Question	Answer
DOC-1	Manufacturer Name	See last page
DOC-2	Device Description	Digital mammography
DOC-3	Device Model	MAMMOMAT B.brilliant
DOC-4	Document ID	Internal ID
DOC-5	Manufacturer Contact Information	See last page
DOC-6	Intended use of device in network-connected environment:	See section "Basic information"
DOC-7	Document Release Date	2023
DOC-8	Coordinated Vulnerability Disclosure: Does the manufacturer have a vulnerability disclosure program for this device?	Yes, see 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, Siemens Healthineers is part of Health-ISAC.
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

Question ID	Question	Answer	See note
	Management of personally identifiable information (MPII)		
MPII-1	Can this device display, transmit, store, or modify personally identifiable information (e.g., electronic Protected Health Information (ePHI))?	Yes	
MPII-2	Does the device maintain personally identifiable information?	Yes	
MPII-2.1	Does the device maintain personally identifiable information temporarily in volatile memory (i.e., until cleared by power-off or reset)?	Yes	
MPII-2.2	Does the device store personally identifiable information persistently on internal media?	Yes	
MPII-2.3	Is personally identifiable information preserved in the device's non-volatile memory until explicitly erased?	Yes	
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 information after it is stored to a long term solution?	Yes	
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	
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)?	Yes	1
MPII-3	Does the device have mechanisms used for the transmitting, importing/exporting of personally identifiable information?	Yes	

Manufacturer Disclosure Statement (MDS²)

Question ID	Question	Answer	See note
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	2
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	
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	3
MPII-3.8	Does the device import personally identifiable information via scanning a document?	Yes	4
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?	No	

MPII notes:

1. Possible to export ePHI/PII data to configured media
2. Import/export of private data is possible via the following removable media: CD/DVD, USB device (memory stick, portable disk). Both functions can be disabled on service level.
3. Communication with RIS and PACS within the hospital network. Communication with SRS does not contain PII.
4. Barcode scanning within patient registration

Question ID	Question	Answer	See note
	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.		
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	1
ALOF-2	Is the length of inactivity time before auto-logoff/screen lock user or administrator configurable?	Yes	2
	ALOF notes: 1. Available with security option 2. Configurable range: 1–9999 min.		

Question ID	Question	Answer	See note
	Audit Controls (AUDT)		
	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	1
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	
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	

Manufacturer Disclosure Statement (MDS²)

Question ID	Question	Answer	See note
AUDT-2.8.2	Application Programming Interface (API) and similar activity?	No	
AUDT-2.9	Emergency access?	No	2
AUDT-2.10	Other events (e.g., software updates)?	Yes	3
AUDT-2.11	Is the audit capability documented in more detail?	Yes	4
AUDT-3	Can the owner/operator define or select which events are recorded in the audit log?	Yes	
AUDT-4	Is a list of data attributes that are captured in the audit log for an event available?	Yes	4
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?	No	
AUDT-5.3	Via Other communications (e.g., external service device, mobile applications)?	Yes	5
AUDT-5.4	Are audit logs encrypted in transit or on storage media?	No	6
AUDT-6	Can audit logs be monitored/reviewed by owner/operator?	Yes	7
AUDT-7	Are audit logs protected from modification?	Yes	7
AUDT-7.1	Are audit logs protected from access?	Yes	7
AUDT-8	Can audit logs be analyzed by the device?	No	

AUDT notes:

1. Available with security option

2. No emergency access available

3. Audit logs exist for software updates through SRS.

4. See section "Auditing/Logging"

5. Central syslog server is supported.

6. Audit logs stored locally on the system are encrypted. Central auditing is not encrypted.

7. Access controls are in place to provide access for authorized personnel only.

Question ID	Question	Answer	See note
	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
AUTH-1.1	Can the device be configured to use federated credentials management of users for authorization (e.g., LDAP, OAuth)?	Yes	2
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)?	No	
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	
	AUTH notes: 1. Available with security option 2. Microsoft Active Directory integration supported		

	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.		
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 2.1–2.4.	Yes	
CSUP-2.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	No	

Manufacturer Disclosure Statement (MDS^2)

Question ID	Question	Answer	See note
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?	Yes	
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	1
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?	Yes	1
CSUP-4.3	Does the device have the capability to receive remote installation of patches or software updates?	Yes	
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?	No	
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?	Yes	1

Question ID	Question	Answer	See note
CSUP-5.3	Does the device have the capability to receive remote installation of patches or software updates?	Yes	
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 refernce 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?	Yes	1
CSUP-6.3	Does the device have the capability to receive remote installation of patches or software updates?	Yes	
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	
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	2
CSUP-10	Can the owner/operator install manufacturer-approved third-party software on the device themselves?	No	2
CSUP-10.1	Does the system have mechanism in place to prevent installation of unapproved software?	Yes	3
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?	No	
CSUP-11.2	Is there an update review cycle for the device?	No	

Manufacturer Disclosure Statement (MDS^2)

Question ID	Question	Answer	See note
	CSUP notes: 1. Security patches and updates can be installed via Smart Remote Services, by customer via download from teamplay Fleet or by a Siemens Healthineers service technician – depending on the availability of the Smart Remote Services infrastructure at the customer's site and on the impact of the update. 2. The customer is not allowed to install additional third-party software on the system. 3. Microsoft Device Guard disallows the use of non-approved software.		
	Health Data De-Identification (DIDT)		
	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?	Yes	1
DIDT-1.1	Does the device support de-identification profiles that comply with the DICOM standard for de-identification?	Yes	1
	DIDT notes: 1. The de-identification process adheres to DICOM Standard 2016a.		
	Data Backup and Disaster Recovery (DTBK)		
	The ability to recover after damage or destruction of device data, hardware, software, or site configuration information.		
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?	Yes	2, 3
DTBK-4	Does the device have an integral data backup capability to remote storage?	Yes	3
DTBK-5	Does the device have a backup capability for system configuration information, patch restoration, and software restoration?	Yes	4
DTBK-6	Does the device provide the capability to check the integrity and authenticity of a backup?	Yes	5

Question ID	Question	Answer	See note
	DTBK notes: 1. After the factory installation an image of the system software is created, this image can be used as "factory reset". 2. An image of the system software can be backed up to removable media. 3. Backup of patient and image data can be done automatically to an archive system (PACS). The system allows setting up automatic transfer rules so that all acquired images are transferred to a PACS system automatically after each examination. The customer is responsible to set up the transfer rules correctly on the system, so no images are lost in case of system damage or destruction. 4. Backup of the system configuration is done via CD/DVD or USB device through service software. In case of system damage the backup can be restored by Siemens Healthineers service technician after system replacement, system software restoration or system software reinstallation. 5. System configuration backups are protected by a checksum.		
	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.		
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.		
IGAU-1	Does the device provide data integrity checking mechanisms of stored health data (e.g., hash or digital signature)?	No	
IGAU-2	Does the device provide error/failure protection and recovery mechanisms for stored health data (e.g., RAID-5)?	No	
	Malware Detection/Protection (MLDP)		
	The ability of the device to effectively prevent, detect and remove malicious software (malware).		
MLDP-1	Is the device capable of hosting executable software?	No	1
MLDP-2	Does the device support the use of anti-malware software (or other anti-malware mechanism)? Provide details or reference in notes.	Yes	2

Manufacturer Disclosure Statement (MDS²)

Question ID	Question	Answer	See note
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?	No	
MLDP-2.3	Does the device documentation allow the owner/operator to install or update anti-malware software?	No	
MLDP-2.4	Can the device owner/operator independently (re-)configure anti-malware settings?	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?	Yes	3
MLDP-2.7	Are malware notifications written to a log?	Yes	
MLDP-2.8	Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)?	No	
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	2
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?	No	

MLDP notes:

1. Only the system's application software is hosted.
2. Malware protection is based on Microsoft Device Guard (whitelisting) and Microsoft AppLocker.
3. Malware infection is avoided by whitelisting – therefore no repair is needed.

Question ID	Question	Answer	See note
	Node Authentication (NAUT)		
	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)?	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)?	Yes	2
NAUT-2.1	Is the firewall ruleset documented and available for review?	No	
NAUT-3	Does the device use certificate-based network connection authentication?	Yes	3
	NAUT notes: 1. TLS handshake mechanism during secure DICOM transfer ensures node authentication. Trusted host functionality is available to ensure the communication with only the trusted nodes. 2. The Windows firewall is configured to minimize the attack surface. 3. Secure DICOM transfer is supported and is configurable.		

Question ID	Question	Answer	See note
	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.		
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	
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)?	No	
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	

Manufacturer Disclosure Statement (MDS²)

Question ID	Question	Answer	See note
CONN-1.2.3	Does the device require, use, or support removable memory devices?	Yes	1
CONN-1.2.4	Does the device support other physical connectivity?	No	
CONN-2	Does the manufacturer provide a list of network ports and protocols that are used or may be used on the device?	Yes	2
CONN-3	Can the device communicate with other systems within the customer environment?	Yes	2
CONN-4	Can the device communicate with other systems external to the customer environment (e.g., a service host)?	Yes	3
CONN-5	Does the device make or receive API calls?	No	
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	4
CONN-7.1	Is TLS configurable?	Yes	5
CONN-8	Does the device provide operator control functionality from a separate device (e.g., telemedicine)?	No	

CONN notes:

1. Patient data can be imported from/exported to USB storage devices.
2. See section "Network information"
3. The device can connect to Smart Remote Services.
4. TLS 1.2 is supported.
5. DICOM communication can be protected via TLS.
   Communication with Smart Remote Services is protected via TLS.

Person Authentication (PAUT)

The ability to configure the device to authenticate users.

Question ID	Question	Answer	See note
PAUT-1	Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)?	Yes	1, 2, 3
PAUT-1.1	Does the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)?	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.)?	Yes	4

Question ID	Question	Answer	See note
PAUT-3	Is the device configurable to lock out a user after a certain number of unsuccessful logon attempts?	Yes	5
PAUT-4	Are all default accounts (e.g., technician service accounts, administrator accounts) listed in the documentation?	No	
PAUT-5	Can all passwords be changed?	Yes	6
PAUT-6	Is the device configurable to enforce creation of user account passwords that meet established (organization specific) complexity rules?	Yes	7
PAUT-7	Does the device support account passwords that expire periodically?	Yes	8
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	2
PAUT-14.1	Are credentials stored using a secure method?	Yes	2

PAUT notes:

1. Available with security option
2. Windows account management is used.
3. Access to the system via service key is tracked by process.
4. Microsoft Active Directory integration supported
5. Account lockout threshold is configurable.
6. All passwords for user accounts can be changed. Passwords of functional accounts which are only used for internal services can be resetted to new random passwords.
7. Complexity rules are configurable.
8. Expiration time is configurable. Does not apply the functional accounts which are only used for internal services.

Manufacturer Disclosure Statement (MDS²)

Question ID	Question	Answer	See note
	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		
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, 2
PLOK-3	Are all device components maintaining personally identifiable information (other than removable media) physically secured behind an individually keyed locking device?	Yes	1, 3
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. The customer is responsible for the physical protection. 2. The AWS PC is mounted in a case in the control table (optional). 3. The AWS PC case can be locked with an ordinary Kensington lock.		

Question ID	Question	Answer	See note
	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.		
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	1
RDMP-3	Does the manufacturer maintain a web page or other source of information on software support dates and updates?	Yes	
RDMP-4	Does the manufacturer have a plan for managing third-party component end-of-life?	Yes	
	RDMP notes: 1. Third-party SW is hardened according to guidelines provided by the supplier. Additionally it is hardened according to DISA STIGs if available.		

Question ID	Question	Answer	See note
	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?	Yes	1
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?	No	
SBOM-3	Does the device include a command or process method available to generate a list of software components installed on the device?	Yes	2
SBOM-4	Is there an update process for the SBoM?	Yes	
	SBOM notes: 1. See section “Software bill of materials” 2. Can be delivered on special request		

Question ID	Question	Answer	See note
	System and Application Hardening (SAHD)		
	The device’s inherent resistance to cyber attacks and malware.		
SAHD-1	Is the device hardened in accordance with any industry standards?	Yes	1
SAHD-2	Has the device received any cybersecurity certifications?	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	3
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	3

Manufacturer Disclosure Statement (MDS²)

Question ID	Question	Answer	See note
SAHD-4	Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)?	No	
SAHD-5	Is the system configurable to allow the implementation of file-level, patient level, or other types of access controls?	Yes	4
SAHD-5.1	Does the device provide role-based access controls?	Yes	4
SAHD-6	Are any system or user accounts Unrestricted or disabled by the manufacturer at system delivery?	Yes	5
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?	Yes	
SAHD-7	Are all shared resources (e.g., file shares) which are not required for the intended use of the device disabled?	Yes	6
SAHD-8	Are all communication ports and protocols that are not required for the intended use of the device disabled?	Yes	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?	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?	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	9
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	10
SAHD-14	Can the device be hardened beyond the default provided state?	No	
SAHD-14.1	Are instructions available from vendor for increased hardening?	No	
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	

Question ID	Question	Answer	See note
	SAHD notes: 1. STIGs provided by IASE DISA are considered for hardening. 2. Microsoft Device Guard 3. Microsoft Device Guard prevents execution of unsigned binaries. 4. Available with security option 5. Built-in administrator account and Guest account are disabled. 6. No shared resources are provided. 7. See list of open ports in section "Network information" 8. All services that are not used are disabled. 9. Boot of external media is protected by a BIOS password. 10. To ensure patient safety, scanning of this device is not allowed during clinical use. It is strongly recommended to reboot the system after the scan is finished.		
	Security Guidance (SGUD)		
	Availability of security guidance for operator and administrator of the device and manufacturer sales and service.		
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	1
SGUD-3	Are all access accounts documented?	No	
SGUD-3.1	Can the owner/operator manage password control for all accounts?	Yes	2
SGUD-4	Does the product include documentation on recommended compensating controls for the device?	Yes	3
	SGUD notes: 1. Available for Service Personnel in Service Documentation 2. All passwords for user accounts can be changed. Passwords of functional accounts which are only used for internal services can be reset to new random passwords. 3. See section "Boundary defense"		

Manufacturer Disclosure Statement (MDS²)

Question ID	Question	Answer	See note
	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.		
STCF-1	Can the device encrypt data at rest?	No	
STCF-1.1	Is all data encrypted or otherwise protected?	Yes	1
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?	N/A	
STCF-3	Is the data stored in a database located on the device?	Yes	2
STCF-4	Is the data stored in a database external to the device?	No	

STCF notes:

1. Patient data is protected by role-based access control and auditing of PHI access is supported (available with security option).
2. Initially the data is stored in a local database on the device. It is recommended to store the patient data on the PACS right after the examination is finished.

Question ID	Question	Answer	See note
	Transmission Confidentiality (TXCF)		
	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?	No	
TXCF-2	Is personally identifiable information encrypted prior to transmission via a network or removable media?	No	1, 2
TXCF-2.1	If data is not encrypted by default, can the customer configure encryption options?	Yes	3
TXCF-3	Is personally identifiable information transmission Unrestricted to a fixed list of network destinations?	Yes	4
TXCF-4	Are connections limited to authenticated systems?	No	3, 4
TXCF-5	Are secure transmission methods supported/implemented (DICOM, HL7, IEEE 11073)?	Yes	1

Question ID	Question	Answer	See note
	TXCF notes: 1. Secure DICOM is supported. 2. Data exported to removable media is not encrypted. Central auditing feature communication is not encrypted. 3. Secure DICOM can be activated. 4. DICOM communication is restricted to configured network nodes ("trusted hosts").		
	Transmission Integrity (TXIG)		
	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?	Yes	1, 2
TXIG-2	Does the device include multiple sub-components connected by external cables?	Yes	3
	TXIG notes: 1. Software updates are digitally signed. Any modification would result in invalid binaries, which would be rejected by the whitelisting. 2. Secure DICOM is supported. Any modification during transport would be detected. 3. See section "Network information"		
	Remote Service (RMOT)		
	Remote service refers to all kinds 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?	Yes	1
RMOT-1.1	Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair?	Yes	2
RMOT-1.2	Is there an indicator for an enabled and active remote session?	Yes	3
RMOT-1.3	Can patient data be accessed or viewed from the device during the remote session?	Yes	4
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	5

Manufacturer Disclosure Statement (MDS²)

Question ID	Question	Answer	See note
	RMOT notes:		

1. Depending on the availability of the Smart Remote Services infrastructure at the customer's site
2. A user can initiate a remote assistance session. A user can grant limited or full access to a service technician for using the web service of the device.
3. A remote assistance session is indicated by the TeamViewer application.
   A remote session with limited access via the webservice is indicated via an icon in the status bar.
   A remote session with full access is indicated by a lock screen preventing the user from working.
4. After the user has initiated a remote assistance session via TeamViewer and granted control to the remote service technician, that service technican could see patient data residing on the system.
5. Software updates via Smart Remote Service

Other Security Considerations (OTHR)

None

Manufacturer Disclosure Statement (IEC 60601-1)

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; 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: • changes in NETWORK/DATA COUPLING configuration; • connection to additional items to the NETWORK/DATA COUPLING; • disconnecting items from the NETWORK/DATA COUPLING; • update of equipment connected to the NETWORK/DATA COUPLING; • upgrade of equipment connected to the NETWORK/DATA COUPLING
Z1 notes:	N/A

Z2. Intended purpose of integrating the device into an IT network	
Z2-1	This Siemens Healthineers product is designed as a Mammography image acquisition system in order to acquire X-ray images of the human breast for screening and diagnostic pruposes. Depending on enabled options it can also be used for image-guided biopsies.
Z2-2	The system consists of the following components:
Z2-2.1	Mammography unit stand with X-ray tube and digital X-ray detector
Z2-2.2	Acqusition workstation consisting of a PC with Windows 10 operating system.
Z2-2.3	In addition to the underlying operating system, a proprietary operative system (*syngo*) is running on the acquisition workstation.
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	Beside the DICOM interface the system does not provide third-party software interfaces.
Z2-6	The system provides remote assistance functionality, which enables the user to gather support via the common Remote Service Platform.
Z2 notes:	N/A

Manufacturer Disclosure Statement (IEC 60601-1)

Z3. Network properties required by the system and resulting risks	
Z3-1	Ethernet Connection of the clinical Network (TCP/IP, 1 Gbit/s)
Z3-1.1	If the network is down, network services (see below) are 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 (1 Gbit/s) is not provided, the transfer of images is prolonged 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.
Z3-1.6	A failure of the IT-NETWORK (e.g., the intrusion of malware) might result in hazardous situations affecting the confidentiality, integrity and availability of image and reporting data. These possible risks have been identified: • unavailability or loss of image or patient data • modification of images or patient data • modification of imaging or image processing parameters • other unexpected system behaviour
Z3-2	PACS 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 unarchived images can be lost.
Z3-2.2	If the PACS is not available, images cannot be archived after the examination. Examinations may be no longer possible because the hard disk is full (because unarchived images cannot be automatically removed).
Z3-2.3	If the PACS is not available, images cannot be archived after the examination. In case of manual deletion of images, unarchived 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 subsequent to the last transfer operations is prolonged.
Z3-3	DICOM Printer
Z3-3.1	If the DICOM printer is not available, film is not available for diagnosis/archive.

Z3. Network properties required by the system and resulting risks	
Z3-4	RIS
Z3-4.1	If the RIS is not available, modality worklist is not available. This can lead to data inconsistencies.
Z3-4-2	If the RIS is not available, modality worklist is not available. This can result in images sent to PACS not being available until they are manually synchronized with the RIS data.
Z3-4.3	If a reduced network performance is compensated with a long Worklist Query time-out, this could result in outdated RIS data being used to register a patient from the scheduled list on the system.
Z3-5	Network Connection to Siemens Healthineers Remote Service Server
Z3-5.1	If the connection to the Remote Service Server is not available, software patches cannot be distributed.
Z3-5.2	If the connection to the Remote Service Server is not available, Siemens Healthineers support is restricted.
Z3 notes:	N/A

Abbreviations

AWS	Acquisition Workstation
BIOS	Basic Input Output System
DHCP	Dynamic Host Configuration Protocol
DICOM	Digital Imaging and Communications in Medicine
DISA	Defense Information Systems Agency
DMZ	Demilitarized Zone
DNS	Domain Name System
ePHI	Electronic Protected Health Information
FDA	Food and Drug Administration
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
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
HIS	Hospital Information System
IASE	Information Assurance Support Environment
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IPS	Intrusion Prevention System
LDAP	Lightweight Directory Access Protocol
MDS^2	Manufacturer Disclosure Statement for Medical Device Security
NEMA	National Electrical Manufacturers Association
NTP	Network Time Protocol
OCR	Office for Civil Rights
PACS	Picture Archiving and Communication System
PHI	Protected Health Information
PII	Personally Identifiable Information
RIS	Radiology Information System
SBoM	Software Bill of Material
SHA	Secure Hash Algorithm
SRS	Smart Remote Services
STIGs	Security Technical Implementation Guides
SW	Software
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
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

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 white paper are designed to describe Siemens Healthineers’ approach to cybersecurity of its medical devices and to disclose the security capabilities of the devices/systems described herein. Neither Siemens Healthineers nor any medical device manufacturer can warrant that its systems will be invulnerable to cyberattack. Siemens Healthineers makes no representation or warranty that its cybersecurity efforts will ensure that its medical devices/systems will be error-free or secure against cyberattack.

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

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

Published by Siemens Healthcare GmbH · 13246 0623 online · © Siemens Healthcare GmbH, 2023