White Paper

MAX Systems (VF10)

Product & Solution Security Whitepaper and MDS2 Form

The facts about the security of our products and solutions.

VF10 SW version is 510(k) pending and is not yet commercially available in the United States.

siemens.com/healthineers

SIEMENS Healthineers

Introduction

The Siemens Healthcare product security program

At Siemens Healthcare, we are committed to working with our customers to address their security and privacy requirements. Our Product and Solution Security Office is responsible for our global program so that security is addressed throughout the life-cycle of our medical devices.

Our program addresses state of the art security in our current and future products and appropriately addresses legacy products that were in the field before the program was established. We support our customers to protect the privacy of their data at the same time providing measures that strengthen the resiliency of our products from external cyber-security attackers.

We comply with security and privacy regulations from the US Department of Health and Human Services (HHS), including the Food and Drug Administration (FDA) and Office for Civil Rights (OCR), to help our customers meet their own IT security and privacy obligations.

Vulnerability and incident management

Siemens actively monitors reported potential vulnerabilities and incidents from sources including customers, vendors, security researchers and government agencies. We cooperate with these entities when addressing these reports.

Our communications policy is one of responsible cooperate. We work in this way with our customers and other parties, when appropriate, in response to potential vulnerabilities and incidents in our medical devices, no matter what the source.

Elements of our security program for MAX VF10 systems

- Providing information to customers about the secure configuration and use of our medical devices in their IT environment
- Formal threat and risk analysis for our medical devices
- Secure architecture, design and coding methodologies in our software development process
- Automated code analysis of medical device software
- Patch management tailored to the medical device and customer needs
- Security testing of medical devices under development as well as medical devices already in the field
- Security vulnerability monitoring to track reported third party components issues in our medical devices
- Working with our supplier to address security throughout the supply chain
- Employee training for consistent knowledge with the requirements to contribute to protecting our customers' data and security

Contacting Siemens Healthcare about product security

Siemens Healthcare requests that any security or privacy incidents be reported by email to:

productsecurityreporting.healthcare@siemens.com

For all other communication with Siemens Healthcare about product security:

cpssos.healthcare@siemens.com

VF10 SW version is 510(k) pending and is not yet commercially available in the United States.

MAX Systems Basic Information

Ysio Max

Luminos dRF Max

Uroskop Omnia Max

Luminos Agile Max

Multitom Rax

Function and purpose of the products

- **Ysio Max** is a diagnostic imaging system for radiographic studies. Typical examinations are X-ray exposures of the head, spinalcolumn, abdomen, thorax (lungs), internal organs and extremities.
- The **Luminos dRF Max** and **Luminos Agile Max** are diagnostic imaging systems for radiographic and fluoroscopic studies. Typical examinations are gastrointestinal examinations or cranial, skeletal thoracic and lung exposures.
- **Multitom Rax** is a digital, detector-based X-ray scanner that provides X-ray based imaging, interventions and therapeutic procedures in the area of radiography, fluoroscopy, orthopedics, selected angiography, trauma and 3D volume imaging.
- The **Uroskop Omnia Max** is a X-ray system for urological diagnosis and the support of urological therapeutic applications. Typical examinations are transurethral interventions and Urological X-ray diagnosis.

VF10 SW version is 510(k) pending and is not yet commercially available in the United States.

MAX Systems Network Diagram

Overview how the MAX systems exist in a hospital environment

The MAX systems are integrated into the hospital network environment as shown in the following figures.

Ysio Max

X-ray room with table and wall stand set up (Example – other configurations available).

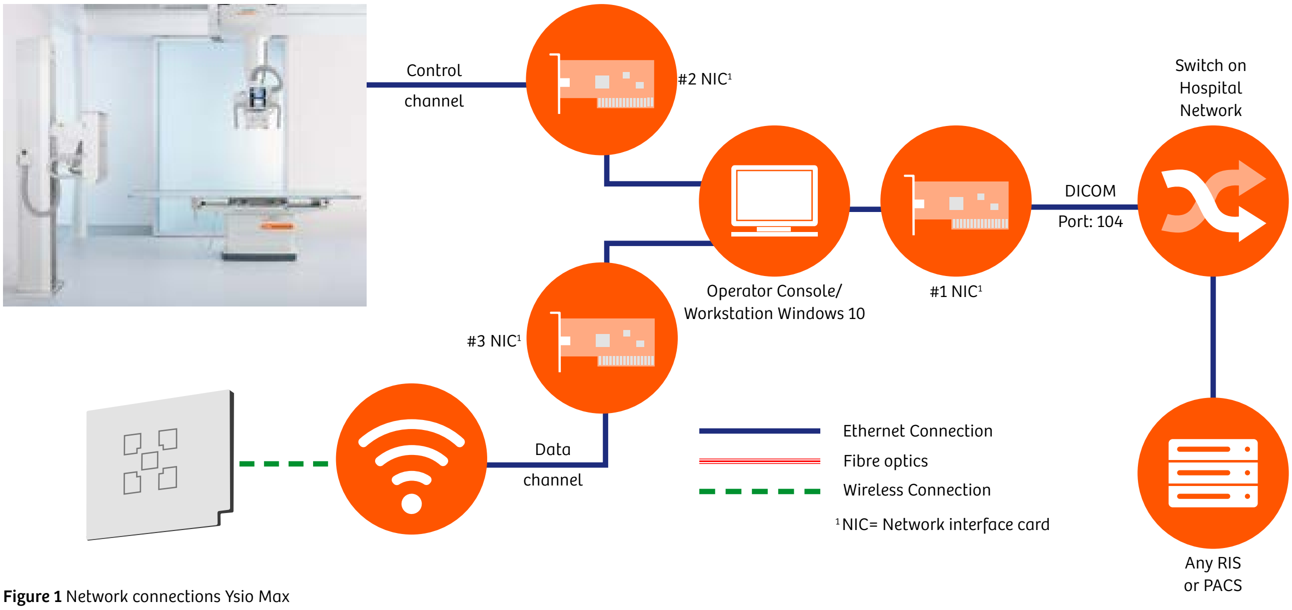

Figure 1 Network connections Ysio Max

VF10 SW version is 510(k) pending and is not yet commercially available in the United States.

Luminos Agile Max/Luminos dRF Max

RF room with monitors, table and wall stand set up (Example – other configurations available).

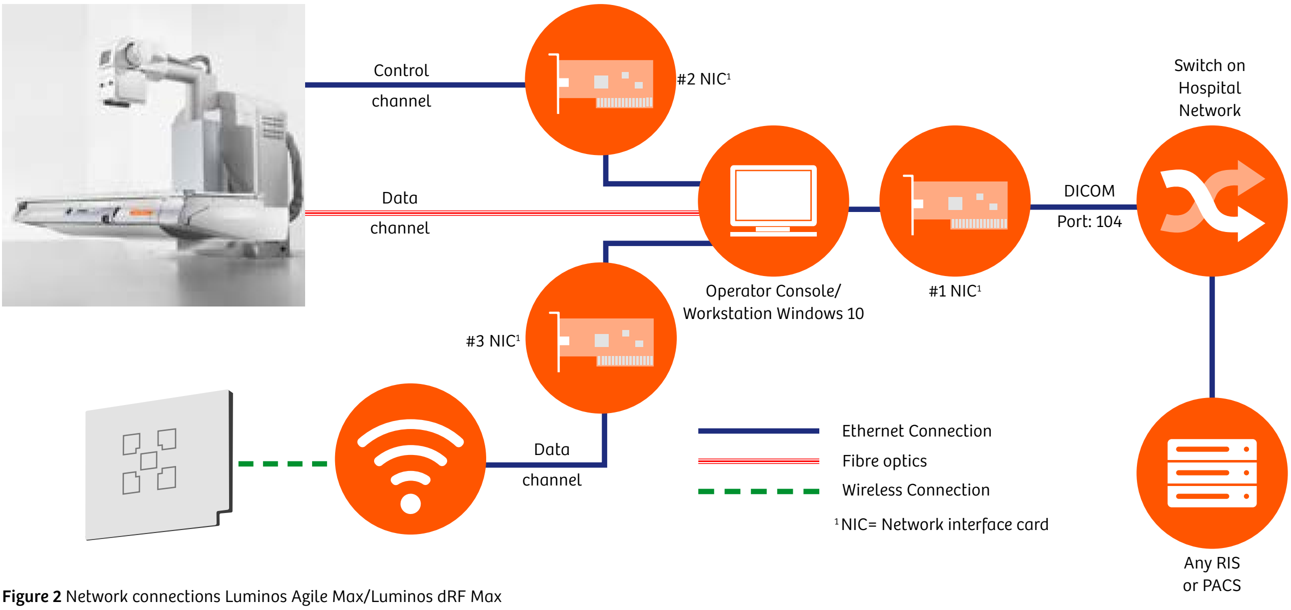

Figure 2 Network connections Luminos Agile Max/Luminos dRF Max

Uroskop Omnia Max

Urology system with table and monitor set up.

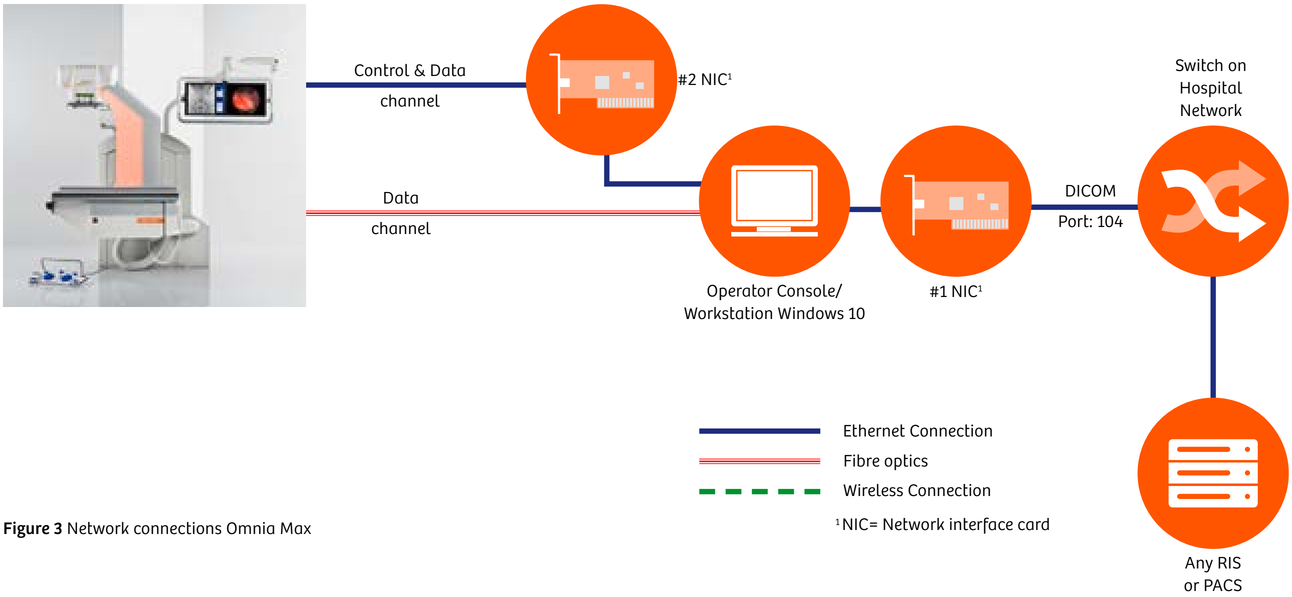

Figure 3 Network connections Omnia Max

VF10 SW version is 510(k) pending and is not yet commercially available in the United States.

Multitom Rax

RF room with monitors, table and wall stand set up (Example – other configurations available).

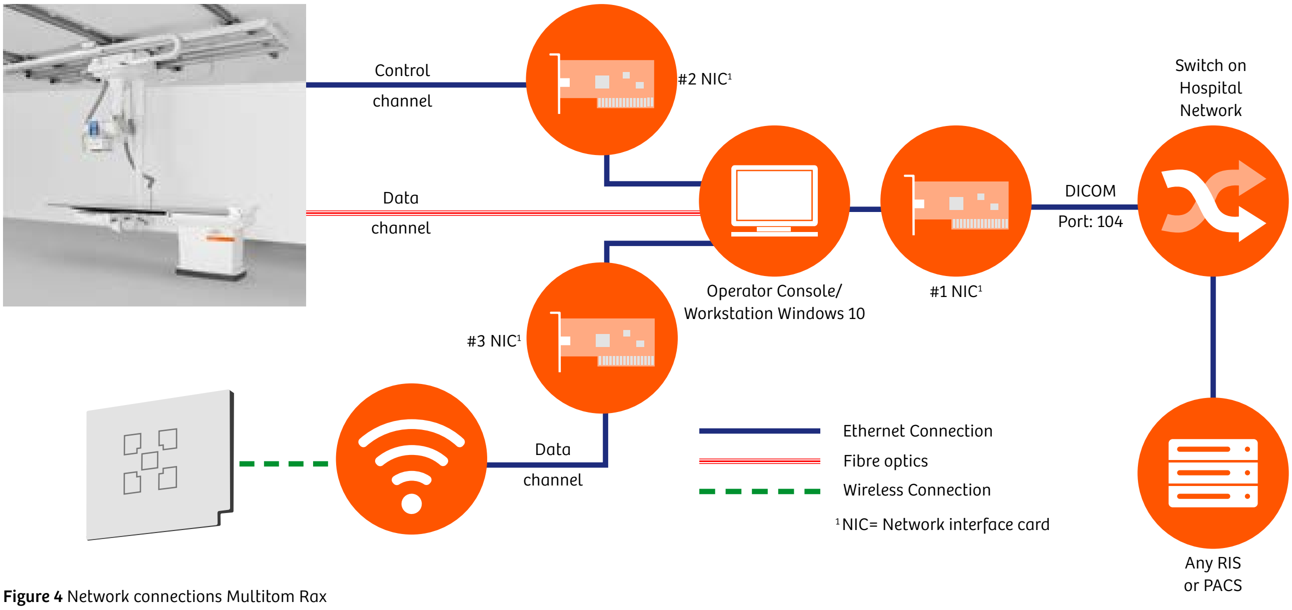

Figure 4 Network connections Multitom Rax

VF10 SW version is 510(k) pending and is not yet commercially available in the United States.

MAX Systems Security Controls

Inventory of Devices

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

Internally the *syngo* FLC is connected to X-ray generator and mechanical system via a proprietary protocol based on Ethernet. Additionally the *syngo* FLC is internally connected to X-ray detectors. This can be a wired or a wireless (WLAN) connection.

For details see Figure 1 to Figure 4.

Inventory of Software

syngo FLC integrates off the shelf software applications which are being actively monitored for vulnerabilities. Refer to Appendix II for an excerpt of the list of off the shelf software applications.

Operating Systems

MS Windows 10 Enterprise LTSB

Secure Configurations for Hardware and Software

- Built in firewall is used to minimize the network attack surface.
- System hardening is applied
- Lock of X-ray generator cabinet
- Metal shield on backside of PC in order to hide hardware interfaces

Continuous Vulnerability Assessment and Remediation

Siemens performs vulnerability monitoring of the included third party components (including 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 either installed remotely or on site – depending on the availability of the remote service infrastructure at the customer's site and on the impact of the service pack.

Controlled Use of Administrative Privileges

syngo FLC supports HIPAA (Health Insurance Portability and Accountability Act) regulation with role based privilege assignment and access control. The security option must be procured to enable user management on application level e.g. routine clinical user, emergency user, administrator.

Web Browser Protections

syngo FLC supports built in Internet explorer. Webbrowser is only accessible for the service technician. Access is limited to trusted websites.

Malware Defense

syngo FLC employs tools for malware defense:

- Whitelisting: Device Guard.
- Microsoft Firewall.

Firewall rules are configured so that inbound connections from devices are restricted to minimize the attack surface.

VF10 SW version is 510(k) pending and is not yet commercially available in the United States.

Limitation and Control of Network Ports, Protocols, and Services

syngo FLC uses the Windows firewall to restrict access.
The following ports are needed by the Max Products and need to be opened in the hospital network firewall:

Application	Functionality	Network -> *syngo* FLC (In-going)	*syngo* FLC -> network (Out-going)
Windows operating system	DNS	None	53 (UDP, TCP)
	DHCP	None	67 (UDP)
	NTP	None	123 (UDP)
	Kerberos	None	88 (UDP, TCP)
DICOM	DICOM	104, 2762 (TCP)	Configurable by customer (TCP)
Audit Trail	Centralized logging	5985 (TCP)	None
Remote Services	MNP	8226, 13001 (TCP)	8227, 8228, 12061 (TCP)
	Teamviewer	11080, 11081 (TCP)	None
	Transfermanager	49152 - 65534 (TCP)	20-21 (TCP)
	Remote Web Service	443 (TCP)	None

Ports for DICOM communication are opened for configured peer nodes, e.g. PACS (picture archiving and communication system) or RIS.

VF10 SW version is 510(k) pending and is not yet commercially available in the United States.

Recovery Capability

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

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

Boundary Defense

Built in firewall is used to minimize the network attack surface.

For optimized protection of sensitive data and operation of the system it must be deployed in a secure network environment, utilizing e.g. network segmentation, client access control and protection against access from public networks.

Boundary defenses in the hospital should be multilayered relying on firewalls, proxies, DMZ[1] and network based IDS[2] and IPS[3].

Data Protection

Personal Health Information (PHI) is protected by role based access control. Data at rest is protected by hard disk encryption. Data in transit can be protected by DICOM encryption. The security option must be procured to support this.

Controlled Access Based on the Need to Know

syngo FLC supports HIPAA (Health Insurance Portability and Accountability Act) standard with role based privilege assignment and access control. The security option must be procured to support this.

Wireless Access Control

The MAX systems (except of Uroskop Omnia Max) provide a private WLAN network to connect their portable detectors. WPA2 encryption is enforced for this WLAN using a random-generated site-specific password. No Personal Health Information (PHI) is transmitted via this WLAN.

Account Monitoring and Control

System Administrator must manage the lifecycle of system accounts, their creation, use, dormancy, deletion in order to minimize opportunities for attackers to leverage the system.

Security Skills Assessment and Appropriate Training to Fill Gaps

The configuration of the role based privilege assignment and access control is described in the user manual.

Security training is provided and mandatory for all involved employees. In addition, security experts and responsible persons are nominated and specially qualified.

Incident Response and Management

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

[1]DMZ = Demilitarized zone

[2]IDS = Intrusion detection system

[3]IPS= Intrusion prevention system

[4]MNP= Managed Node Package

VF10 SW version is 510(k) pending and is not yet commercially available in the United States.

Appendix I

Content of Audit Trail

The audit file includes a header showing the start date and logs at every system startup:

- Dicom AETs
- Location
- Institution
- IP address
- Host ID
- SerialNumber
- FLC software version
- ProductName (“Fluorospot Compact”)
- VendorName (“SIEMENS”)

The following events are logged:

- User login (including emergency user login) and logout (date+time, user)
- Failed login attempts (date+time, user, failure cause)
- Create patient or study (by user or RIS) (date+time, user, patient name, patient id, patient sex, patient date of birth)
- Update patient information (date+time, user, patient name, patient id, patient sex, patient date of birth)
- Delete images (date+time, user, patient name, patient id, number of deleted unarchived images)
- Close study (date+time, user, patient name, patient id, number of new images)
  - Acquired or stored images in patient study when patient is closed (deselected) and new images were added (independent if new x-ray was performed or images were changed and stored)
- Delete study (date+time, user, patient name, patient id)
- R/L marker set and delete (date+time, user, patient name, patient id, action, image uid)
- CD Write (date+time, user, patient name, study uid)
- Query/Retrieve (date+time, user, image server AET, patient name, patient id, patient sex, patient date of birth)
- Paper-print (date+time, user, patient name, image number, destination, format and size)
- Dicom print (date+time, user, patient name, image number, destination, format and size)
- Dicom send (date+time, user, patient name, image number and uid, destination)
- Service session start and end (date+time, user, service session id)
- Access to operating system (date+time)
- Access via remote service (date+time, user, service session id)Access to user management
- User account creation/deletion/modification
- User account enabling/disabling
- User group modification, creation and deletion
- Backup/restore of user groups
- Creation of an administrator account
- Updated assignment of users to groups

VF10 SW version is 510(k) pending and is not yet commercially available in the United States.

- Access to the rejected image statistics
- Access to the audit logs via the local viewer
- Export of the audit logs
- Manual deletion of audit logs
- Changes in the audit log configuration
- Access to quality functions: EXI logs/quality control study/study statistics./LUT Editor
- Added or modified worklist entry
- Refused DICOM connection
- Received Storage Commitment
- Image acquisition, deletion or creation via store button
- Main postprocessing actions after the image has been stored
- Executed functions which depend on a HIPAA privilege
- Enable/Disable antivirus scan
- Changes in the whitelisting configuration (DeviceGuard)
- Encryption or decryption of the hard disk (Bitlocker)
- Reboot
- Service activities
- Automatic or manual selection of an OGP
- Creation, modification and deletion of an OGP
- Overwriting acquisition parameters
- Export, import, merge of the PEX database
- Availability of the emergency user
- Hardening/Unhardening of OS
- Reset of passwords
- Password complexity settings: Length x, history y, upper z, lower a, numeric b, special c
- Screensaver timer configuration
- Regarding certificate configuration:
  selection of "Import intermediate/root certificate",
  "Import certificate for DICOM secure connection",
  "Reset to self-signed certificate"
  and "Export self-signed certificate"
- Regarding virtualization: Enable USB/DVD (yes/no) and device unit
- Changes at user settings for:
  Image Delete/Examination/Acquisition Order/Image Display/Print/Exam manager/DICOM Properties/Patient Registration/Site Info

VF10 SW version is 510(k) pending and is not yet commercially available in the United States.

Appendix II

Off the Shelf software's integrated (excerpt).

SW Component	Manufacturer
ActiveMQ	The Apache Software Foundation
Apache Tomcat	The Apache Software Foundation
BIOS	Fujitsu
Hibernate	Red Hat
jQuery	jQuery Foundation
Radia	Accelerite
Managed Node Package (MNP)	Hewlett Packard
Merge Toolkit	Merge
Microsoft .NET	Microsoft
MS VisualC++ 2010 Redistributable	Microsoft
Net-SNMP	Net-SNMP
Nvidia CUDA	Nvidia
Nvidia Graphics adapter Driver	Nvidia
Pixrad	Thales
pdf.js	Mozilla Foundation
Spring Framework	SpringSource
Struts 2	The Apache Software Foundation
Teamviewer	Teamviewer
Windows 10	Microsoft
Zulu Java	Azul Systems

VF10 SW version is 510(k) pending and is not yet commercially available in the United States.

MAX Systems MDS2 Form

	Manufacturer Disclosure Statement for Medical Device Security – MDS^{2}		
	MANAGEMENT OF PRIVATE DATA		
	Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #
A	Can this **device** display, transmit, or maintain **private data** (including **electronic Protected Health Information** [ePHI])?	Yes	_
B	Types of **private data** elements that can be maintained by the **device**:		
B.1	Demographic (e.g., name, address, location, unique identification number)?	Yes	_
B.2	Medical record (e.g., medical record #, account #, test or treatment date, **device** identification number)?	Yes	_
B.3	Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)?	Yes	_
B.4	Open, unstructured text entered by device user/operator?	Yes	1
B.5	**Biometric data**	No	_
B.6	Personal financial information?	No	_
C	Maintaining **private data** - Can the **device**:		
C.1	Maintain **private data** temporarily in volatile memory (i.e., until cleared by power-off or reset)?	Yes	_
C.2	Store **private data** persistently on local media?	Yes	_
C.3	Import/export **private data** with other systems?	Yes	_
C.4	Maintain **private data** during power service interruptions?	Yes	_
D	Mechanisms used for the transmitting, importing/exporting of **private data** – Can the **device**:		
D.1	Display private data (e.g., video display, etc.)?	Yes	_
D.2	Generate hardcopy reports or images containing private data?	Yes	_
D.3	Retrieve **private data** from or record **private data** to **removable media** (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick, etc.)?	Yes	_
D.4	Transmit/receive or import/export **private data** via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire, etc.)?	Yes	_
D.5	Transmit/receive **private data** via a wired network connection (e.g., LAN, WAN, VPN, intranet, Internet, etc.)?	Yes	2
D.6	Transmit/receive **private data** via an integrated wireless network connection (e.g., WiFi, Bluetooth, infrared, etc.)?	No	_
D.7	Import **private data** via scanning?	No	
D.8	Other?	N/A	
	1) Text/comment can be applied to images. 2) Import/export of private data is possible via the following removable media: CD/DVD, USB device (memory stick, portable disk). 3) Medical images are transferred via WLAN without assignment to private patient data 4) Mobilett Mira Max supports transfer of private data via the hospital WiFi		

Management of Private Data notes:

VF10 SW version is 510(k) pending and is not yet commercially available in the United States.

	SECURITY CAPABILITIES		
	Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #
1	**AUTOMATIC LOGOFF (ALOF)** The **device's** ability to prevent access and misuse by unauthorized **users** if **device** is left idle for a period of time.		
1-1	Can the **device** be configured to force reauthorization of logged-in **user(s)** after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)?	Yes	_
1-1.1	Is the length of inactivity time before auto-logoff/screen lock **user** or administrator configurable? (Indicate time [fixed or configurable range] in notes.)	Yes	1
1-1.2	Can auto-logoff/screen lock be manually invoked (e.g., via a shortcut key or proximity sensor, etc.) by the **user**?	Yes	_
ALOF Notes	1) configurable range (0-99 min.)		
2	**AUDIT CONTROLS (AUDT)** The ability to reliably audit activity on the **device**.		
2-1	Can the medical **device** create an **audit trail**?	Yes	1
2-2	Indicate which of the following events are recorded in the audit log:		
2-2.1	Login/logout	Yes	2
2-2.2	Display/presentation of data	No	_
2-2.3	Creation/modification/deletion of data	Yes	2
2-2.4	Import/export of data from **removable media**	Yes	2
2-2.5	Receipt/transmission of data from/to external (e.g., network) connection	Yes	2
2-2.5.1	Remote service activity	Yes	2
2-2.6	Other events? (describe in the notes section)	Yes	2
2-3	Indicate what information is used to identify individual events recorded in the audit log:		
2-3.1	User ID	Yes	_
2-3.2	Date/time	Yes	_
AUDT notes:	1) Available with security option 2) Refer to apendix I		

VF10 SW version is 510(k) pending and is not yet commercially available in the United States.

	Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #
3	**AUTHORIZATION (AUTH)** The ability of the **device** to determine the authorization of users.		
3-1	Can the **device** prevent access to unauthorized **users** through **user** login requirements or other mechanism?	Yes	1
3-2	Can **users** be assigned different privilege levels within an application based on 'roles' (e.g., guests, regular **users**, power **users**, administrators, etc.)?	Yes	1
3-3	Can the **device** owner/**operator** obtain unrestricted administrative privileges (e.g., access operating system or application via local root or admin account)?	No	2
AUTH notes	1) Available with security option 2) Unlimited access to the operating system is not possible for customer personel - even for the user administrator. Only trained Siemens service personel can gain access to the operating system		
4	**CONFIGURATION OF SECURITY FEATURES (CNFS)** The ability to configure/re-configure **device security capabilities** to meet **users'** needs.		
4-1	Can the **device** owner/operator reconfigure product **security capabilities**?	Yes	1
CNFS notes:	1) Available with security option: User accounts and their accessibility can be configured by administrator.		
5	**CYBER SECURITY PRODUCT UPGRADES (CSUP)** The ability of on-site service staff, remote service staff, or authorized customer staff to install/upgrade **device's** security patches.		
5-1	Can relevant OS and **device** security patches be applied to the **device** as they become available?	See Note	1
5-1.1	Can security patches or other software be installed remotely?	Yes	1
CSUP notes:	1) Siemens performs vulnerability monitoring of the included third party components (including 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 either installed remotely or on site by the trained Siemens service technician - depending on the availability of the remote service infrastructure at the customer's site and on the impact of the service pack. Siemens Healthineers performs vulnerability monitoring including 3rd party components continuously. For current version available security patches are distributed to the customer within 90 days from publishing		
6	**HEALTH DATA DE-IDENTIFICATION (DIDT)** The ability of the **device** to directly remove information that allows identification of a person.		
6-1	Does the **device** provide an integral capability to de-identify **private data**?	Yes	_
DIDT notes:	–		
7	**DATA BACKUP AND DISASTER RECOVERY (DTBK)** The ability to recover after damage or destruction of **device** data, hardware, or software.		
7-1	Does the **device** have an integral data backup capability (i.e., backup to remote storage or **removable media** such as tape, disk)?	Yes	1
DTBK notes:	1) Backup of the system configuration is done via HDD or CD/DVD or USB device through service software. In case of system damage the backup can be restored by Siemens service technician after system replacement or re-installation. Backup of patient and image data shall be done automatically to an archive system (PACS). The system allows setting up automatic transfer rules so all acquired images are transfered to a PACS system automatically after each examination. The customer is responsible to set up these transfer rules correctly on the system, so no images will get lost in case of system damage or destruction.		

VF10 SW version is 510(k) pending and is not yet commercially available in the United States.

	Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #
8	**EMERGENCY ACCESS (EMRG)** The ability of **device users** to access **private data** in case of an emergency situation that requires immediate access to stored **private data**.		
8-1	Does the **device** incorporate an **emergency access** ("break-glass") feature?	Yes	1
EMRG notes	1) Available with security option		
9	**HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU)** How the **device** ensures that data processed by the **device** has not been altered or destroyed in an unauthorized manner and is from the originator.		
9-1	Does the **device** ensure the integrity of stored data with implicit or explicit error detection/correction technology?	Yes	1
IGAU notes:	1) Backup of patient and image data shall be done automatically to an archive system (PACS). The system allows setting up automatic transfer rules so all acquired images are transfered to a PACS system automatically after each examination. The customer is responsible to set up these transfer rules correctly on the system, so no images will get lost in case of system damage or destruction.		
10	**MALWARE DETECTION/PROTECTION (MLDP)** The ability of the **device** to effectively prevent, detect and remove malicious software **(malware)**.		
10-1	Does the **device** support the use of **anti-malware** software (or other **anti-malware** mechanism)?	Yes	1
10-1.1	Can the **user** independently re-configure **anti-malware** settings?	No	1
10-1.2	Does notification of **malware** detection occur in the **device user** interface?	Yes	_
10-1.3	Can only manufacturer-authorized persons repair systems when **malware** has been detected?	Yes	1
10-2	Can the device owner install or update anti-virus software?	No	1
10-3	Can the device owner/**operator** (technically/physically) update virus definitions on manufacturer-installed **anti-virus software**?	No	1
MLDP notes:	1) Malware protection is based on Device Guard (Whitelisting).		
11	**NODE AUTHENTICATION (NAUT)** The ability of the **device** to authenticate communication partners/nodes.		
11-1	Does the **device** provide/support any means of node authentication that assures both the sender and the recipient of data are known to each other and are authorized to receive transferred information?	Yes	1
NAUT notes:	1) Authentication of RIS/PACS is supported by means of Dicom Encryption if the security option is provided.		

VF10 SW version is 510(k) pending and is not yet commercially available in the United States.

	Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #
12	**PERSON AUTHENTICATION (PAUT)** The ability of the **device** to authenticate **users**.		
12-1	Does the **device** support **user/operator** -specific username(s) and password(s) for at least one **user**?	Yes	1
12-1.1	Does the device support unique **user/operator** --specific IDs and passwords for multiple users?	Yes	_
12-2	Can the **device** be configured to authenticate **users** through an external authentication service (e.g., MS Active Directory, NDS, LDAP, etc.)?	Yes	1
12-3	Can the **device** be configured to lock out a **user** after a certain number of unsuccessful logon attempts?	Yes	1
12-4	Can default passwords be changed at/prior to installation?	Yes	1
12-5	Are any shared **user** IDs used in this system?	No	_
12-6	Can the **device** be configured to enforce creation of **user** account passwords that meet established complexity rules?	Yes	1
12-7	Can the **device** be configured so that account passwords expire periodically?	Yes	1
PAUT notes	1) Available with security option		
13	**PHYSICAL LOCKS (PLOK)** Physical locks can prevent unauthorized **users** with physical access to the **device** from compromising the integrity and confidentiality of **private data** stored on the **device** or on **removable media**.		
13-1	Are all **device** components maintaining **private data** (other than **removable media**) physically secure (i.e., cannot be removed without tools)?	Yes	_
PLOK notes:	_		
14	**ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP)** Manufacturer's plans for security support of 3rd party components within **device's** life cycle		
14-1	In the notes section, list the provided or required (separately purchased and/or delivered) operating system(s) - including version number(s).	See Note	1
14-2	Is a list of other third party applications provided by the manufacturer available?	Yes	_
RDMP notes:	1) Operating System: MS Windows 10 Enterprise LTSB		

VF10 SW version is 510(k) pending and is not yet commercially available in the United States.

	Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #
15	**SYSTEM AND APPLICATION HARDENING (SAHD)** The device's resistance to cyber attacks and malware.		
15-1	Does the device employ any hardening measures? Please indicate in the notes the level of conformance to any industry-recognized hardening standards.	Yes	1
15-2	Does the device employ any mechanism (e.g., release-specific hash key, checksums, etc.) to ensure the installed program/update is the manufacturer-authorized program or software update?	Yes	1
15-3	Does the device have external communication capability (e.g., network, modem, etc.)?	Yes	2
15-4	Does the file system allow the implementation of file-level access controls (e.g., New Technology File System (NTFS) for MS Windows platforms)?	Yes	_
15-5	Are all accounts which are not required for the intended use of the device disabled or deleted, for both users and applications?	Yes	_
15-6	Are all shared resources (e.g., file shares) which are not required for the intended use of the device , disabled?	Yes	_
15-7	Are all communication ports which are not required for the intended use of the device, disabled?	Yes	_
15-8	Are all services (e.g., telnet, file transfer protocol [FTP], internet information server [IIS], etc.), which are not required for the intended use of the device deleted/disabled?	Yes	_
15-9	Are all applications (COTS applications as well as OS-included applications, e.g., MS Internet Explorer, etc.) which are not required for the intended use of the device deleted/disabled?	Yes	_
15-10	Can the device boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?	No	3
15-11	Can software or hardware not authorized by the device manufacturer be installed on the device without the use of tools?	No	_
SAHD notes	1) Virus protection based on Device Guard (Whitelisting); Firewall is active, dedicated inbound rules, only needed ports are open. Device Guard ensures that unsigned code will not be executed. This functionality can be disabled by a trained Siemens service technician. 2) Ethernet connection 3) Prohibited by BIOS setting, access to BIOS is password protected.		
16	**SECURITY GUIDANCE (SGUD)** The availability of security guidance for operator and administrator of the system and manufacturer sales and service.		
16-1	Are security-related features documented for the device user?	Yes	_
16-2	Are instructions available for device/media sanitization (i.e., instructions for how to achieve the permanent deletion of personal or other sensitive data)?	Yes	_
SGUD notes:	_		

VF10 SW version is 510(k) pending and is not yet commercially available in the United States.

	Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #
17	**HEALTH DATA STORAGE CONFIDENTIALITY (STCF)** The ability of the **device** to ensure unauthorized access does not compromise the integrity and confidentiality of **private data** stored on **device** or **removable media**		
17-1	Can the **device** encrypt data at rest?	Yes	_
STCF notes	–		
18	**TRANSMISSION CONFIDENTIALITY (TXCF)** The ability of the **device** to ensure the confidentiality of transmitted **private data**.		
18-1	Can **private data** be transmitted only via a point-to-point dedicated cable?	No	_
18-2	Is **private data** encrypted prior to transmission via a network or **removable media**? (If yes, indicate in the notes which encryption standard is implemented.)	Yes	2
18-3	Is **private data** transmission restricted to a fixed list of network destinations?	Yes	1
TXCF notes:	1) DICOM Storage Commitment protocol to ensure that receiver takes responsibility of DICOM data transmitted Also encryption available with a security option. 2) Encryption of data in transit: available with security option		
19	**TRANSMISSION INTEGRITY (TXIG)** The ability of the **device** to ensure the integrity of transmitted **private data**.		
19-1	Does the **device** support any mechanism intended to ensure data is not modified during transmission? (If yes, describe in the notes section how this is achieved.)	Yes	1
TXIG notes:	1) Encryption of data in transit; available with security option		
20	**OTHER SECURITY CONSIDERATIONS (OTHR)** Additional security considerations/notes regarding **medical device** security.		
20-1	Can the **device** be serviced remotely?	Yes	_
20-2	Can the **device** restrict remote access to/from specified devices or **users** or network locations (e.g., specific IP addresses)? ?	Yes	_
20-2.1	Can the **device** be configured to require the local **users** to accept or initiate remote access?	Yes	_
OTHR notes:	–		

VF10 SW version is 510(k) pending and is not yet commercially available in the United States.

STATEMENT ACCORDING TO IEC 60601-1; 3rd edition, sub-clause 14.13

1 Instructions for the responsible Organisation

1-1 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

1-2 Subsequent changes to the NETWORK/DATA COUPLING could introduce new RISKS and require additional analysis.

1-3 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

2 Intended purpose of integrating the Device into an IT-Network:

2-1 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.

2-2 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 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 for detailed viewing and long term storage.

3 Network Properties required by the System and resulting risks

3-1 Ethernet Connection of the clinical Network (TCP/IP, 1Gbit/s)

3-1.1 If the network is down, the network service (see below) is not available which can lead to the risks stated below.

3-1.2 If the network is unavailable, medical images can not be transferred for remote consultation.

3-1.3 If the recommended network performance (1Gbit/s) is not provided, the transfer and archiving of images is extended and availability of images at destinations (e.g. for consulting) is delayed.

3-2 PACS system for archiving of Images

3-2.1 If the PACS is not available, images can not be archived after the examination. In case of a system hardware failure all not archived images can be lost.

3-2.2 If the PACS is not available, images can not be archived after the examination. Examinations may be no longer possible because the hard disk is full (because non-archived images can not be automatically removed).

3-2.3 If the PACS is not available, images can not be archived after the examination. In case of manual deletion of images, not archived images can be lost.

3-2.4 If the PACS is not available, images are not available for remote consultation via PACS consoles.

3-2.5 If the PACS is not available, prior images are not available.

3-2.6 If the recommended network performance (1Gbit/s) is not provided, the transfer time to PACS is extended and the time to wait before switching off the System consecutive to last transfer operations is prolonged.

3-3 DICOM Printer

3-3.1 If the DICOM printer is not available, film is not available for diagnose/archive.

3-4 Network Connection to Siemens Remote Service Server

3-4.1 If the connection to the Siemens Remote Service Server is not available, SIEMENS Support is restricted.

VF10 SW version is 510(k) pending and is not yet commercially available in the United States.

Legal Statement

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) 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.

1-3 Any modification of the platform, the software or the interfaces of the device - unless authorized and approved by Siemens AG Healthcare - voids all warranties, liabilities, assertions and contracts.

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.

1-5 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.

VF10 SW version is 510(k) pending and is not yet commercially available in the United States.

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

Published by Siemens Healthcare GmbH · online · 4890 1217 · © Siemens Healthcare GmbH, 2017