White Paper
ACUSON S Family of ultrasound systems,
release VE10

# Security and MDS$^2$ Form

Facts about security and privacy requirements of Siemens Healthineers products and solutions

siemens-healthineers.com/ultrasound

SIEMENS
Healthineers

# The Siemens Healthineers product and solution security program

At Siemens Healthineers, we are committed to working with you to address your cybersecurity and privacy requirements.

Our Product and Solution Security Office is responsible for our global program to ensure that cybersecurity is addressed throughout the lifecycle of our medical devices.

Our product and solution security program addresses state-of-the-art cybersecurity in our current and future products. We support you to protect the privacy of your data, at the same time providing measures that strengthen the resiliency of our products from external cybersecurity attackers.

To help you meet your IT security and privacy obligations, we comply with security and privacy regulations of the U.S. Department of Health and Human Services (HHS), including the Food and Drug Administration (FDA) and Office for Civil Rights (OCR).

### Vulnerability and incident management

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

Our communications policy strives for coordinated disclosure. We work in this way with our customers and other parties, when appropriate, in response to potential vulnerabilities and incidents in our medical devices, no matter the source.

### Elements of our product and solution security program:

- Provide information about the secure configuration and use of Siemens Healthineers medical devices in your IT environment.
- Formal threat and risk analysis for our medical devices.
- Secure architecture, design and coding methodologies in our software development process.
- Static code analysis of medical device software.
- Security testing of medical devices under development as well as medical devices already in the field.
- Patch management tailored to the medical device and your requirements.
- Security vulnerability monitoring to track reported third-party component issues in our medical devices.
- Work with suppliers to ensure security is addressed throughout the supply chain.
- Employee training to ensure their knowledge is consistent with the requirements that contribute to protecting your data and device integrity.

Please contact us anytime to report product and solution security, cybersecurity or privacy incidents, by email to:
productsecurity@siemens-healthineers.com

For all other communications with Siemens Healthineers about product and solution security:
ProductTechnologyAssurance.dl@siemens-healthineers.com

Yours sincerely,

**Jim Jacobson**
Chief Product and Solution Security Officer
Siemens Healthineers

## Contents

**Basic Information** .................................................... 4

**Network Information** ............................................... 5

**Security Controls** ..................................................... 6

**Software Bill of Materials** ........................................ 8

**Manufacturer Disclosure Statement According to IEC60601-1** ......................................... 9

**Manufacturer Disclosure Statement for Medical Device Security – MDS[2]** .............................. 12

**Abbreviations** .......................................................... 19

**Disclaimer According to IEC 80001-1** ....................... 20

**International Electrotechnical Commission Glossary (extract)** ................................................... 20

# Basic Information

## Why is cybersecurity important?

Keeping patient data safe and secure typically should be one of the top priorities of healthcare institutions. It is estimated that the cost associated in the recovery of each medical record in the United States can be as high as $380.[1] According to the Ponemon Institute research report,[2] 39% of medical devices were hacked, with hackers able to take control of the device. Moreover, 38% of healthcare organizations said that their patients received inappropriate medical treatment because of an insecure medical device.

## Our purpose is to make Healthcare providers succeed

The ACUSON S Family™ ultrasound system now features the HELX™ Evolution with Touch Control. The most common request by users was to work with an intuitive, smart ultrasound system that would enable them to manage the need and complexity of caseloads. Siemens Healthineers premium ultrasound system offers unique solutions like elastography imaging, multi-modality review and contrast-enhanced ultrasound to support better imaging and ultrasound assessment by healthcare professionals.

## Operating systems

Please refer to the Software Bill of Materials chapter.

### User account information

- ACUSON S Family systems VE10 software user accounts can be local Windows accounts, managed by the administrator of the system, or LDAP-based accounts if the system is part of a Microsoft Windows Domain.
- A "break-glass" mechanism ensures access to the system in emergency scenarios.
- The system provides preconfigured Password Policies which can be customized by administrators.

### Domain integration

In case of domain integration, it is recommended that the device is put in its own OU. No global policies are allowed. Additional details are provided in the Administration Manual.

## Patching strategy

- Security patches will be provided to maintain the clinical function of the medical device after validation by Siemens Healthineers.
- If connected to Smart Remote Services (SRS), updates can be pushed to the system automatically.
- Technologies and software components are actively monitored for vulnerabilities and availability of security updates.

## Cryptography usage

ACUSON S Family VE10 software utilizes cyphers and protocols built into Windows 7 for encryption and data protection, such as BitLocker for hard drive encryption.

## Handling of sensitive data

- The ACUSON S Family systems are designed for temporary data storage only. Siemens Healthineers recommends storing data to a long-term archive, e.g., on a PACS and shall be deleted in a facility-defined procedure.
- Protected Health Information (PHI) is temporarily stored on the ultrasound system similar to DICOM data, raw data, and meta data for DICOM creation. ***Note:*** *The time for which PHI is stored is determined by the facility.*
- Personally Identifiable Information (PII) as part of the DICOM records also is stored temporarily on the ultrasound system, e.g., patient's name, birthday or age, height and weight, personal identification number, and referring physician's name. Additional sensitive information might be present in user-editable input fields or in the images acquired.
- PHI is transmitted via DICOM – encrypted or unencrypted.

[1] *https://healthitsecurity.com/news/how-much-do-healthcare-databreaches-cost-organizations*

[2] *Ponemon Institute research report, Medical Device Security: An Industry Under Attack and Unprepared to Defend; https://www.ajg.com/media/1699098/medical-devicecybersecuritywhitepaper.pdf*

# Network Information

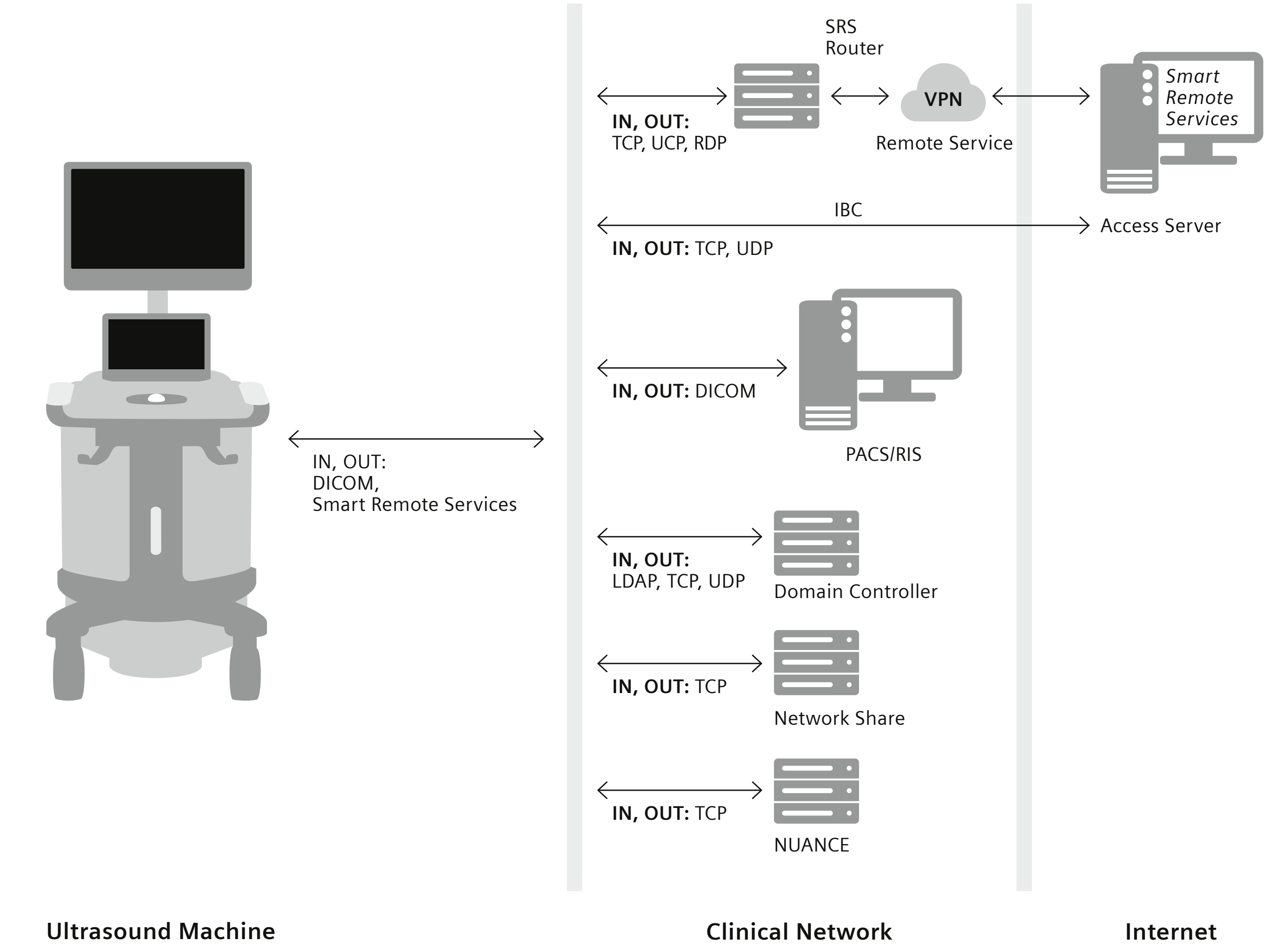

**Figure 1:** System Deployment overview with regard to network boundaries

**Siemens Healthineers recommends operating the ultrasound machine in a dedicated network segment (e.g., VLAN).**

To minimize the risk of unauthorized network access, Siemens Healthineers recommends operating the ultrasound machine behind a firewall and/or use access control lists on the network switches to limit traffic to identified peers. At minimum, the DICOM Port (see Used Port Table below) needs to be visible for customer DICOM network nodes (e.g., PACS, *syngo*®.via etc).

Please contact the Siemens Healthineers Service organization for further information.

The following ports are used by the system:

| Port number | Service/function | Direction | Protocol |
|---|---|---|---|
| **80** | Microsoft IIS1 | Inbound | TCP |
| **104** | DICOM communication (unencrypted) | In/outbound | TCP |
| **443** | Administration Portal – Remote Service (encrypted) | Inbound | TCP |
| **2762** | Secure DICOM (optional) | In/outbound | TCP |
| **8226** | Managed Node Package MNP | Inbound | TCP |
| **8228** | Managed Node Package MNP | Inbound | TCP |
| **11080** | Remote Assist (Team Viewer) | Inbound | TCP |
| **12061** | Managed Node Package MNP | Inbound | TCP |
| **13001** | Managed Node Package MNP | Inbound | TCP |

**Table 1:**
Port Numbers

# Security Controls

### Malware protection

Whitelisting (McAfee® Application Control)

### Controlled use of administrative privileges

The system distinguishes between clinical and administrative roles: clinical users don't require administrative privileges, whereas authorization as the administrator is required for administrative tasks.

### Authentication authorization controls

- ACUSON S Family systems VE10A software supports the Health Insurance Portability and Accountability Act regulation with role-based privilege assignment and access control.
- ACUSON S Family systems VE10A software supports both machine local users and LDAP defined users.
- The user interface of ACUSON S Family systems VE10A software provides a screen lock functionality that can be engaged manually or automatically after a certain amount of inactive time. For details, please refer to the User Manual.

### Vulnerability assessment

Continuous Vulnerability Assessment and Remediation is performed.

### Hardening

ACUSON S Family systems VE10A software hardening is implemented based on the Security Technical Implementation Guidelines developed by the Defense Information Systems Agency (DISA).

### Network controls

- The system is designed to make limited use of network ports and protocols. The Microsoft Windows firewall is configured to block unwanted inbound network traffic except for the ports listed in Table 1.
- Siemens Healthineers recommends operating the system in a secured network environment, e.g., a separate network segmented or a VLAN.
- Connection to the Internet or private networks used by patients/guests is not recommended.
- In case of a denial-of-service (DoS) or malware attack, the system can be taken off the network and operated stand-alone.

### Physical protection

- You are responsible for the physical protection of the ACUSON S Family system's VE10A software, e.g., by installing it in a room with controlled access. Please note that the computer contains patient data and should be protected against tampering and theft.
- It is possible to change the BIOS password. Please contact Siemens Healthineers service for support.

### Data protection controls

- The system is not intended to be an archive (data at rest).
- PHI is protected by both role-based access control as well as hard drive encryption (optional).
- Hard drive encryption is an optional feature that is implemented through Microsoft Bitlocker technology and the usage of the TPM (Trusted Platform Module) chip on the system motherboard.
- The system provides auditing of the PHI access control.
- Optionally, confidentiality and integrity of PHI/PII data can be protected by encryption of DICOM communication with other DICOM nodes.
  ***Note:*** *In VE10 software, the encrypted communication can be used, if all connected DICOM nodes support.*

### Auditing/logging

The system provides HIPAA-compliant auditing of operations on PHI, PII, and user information (e.g., login, read access to PHI, modification of PHI).

### Remote connectivity

SRS is optionally used for proactive maintenance. The connection is created using a secured channel (VPN- or IBC-based). It may be used to download security patches and updates.

### Remote connectivity

The incident handling process is defined and executed on demand to deal with incidents as mandated by the U.S. FDA Post-Market Guidance.

### Incident response and management

The incident handling process is defined and is executed on demand to deal with incidents.

# Software Bill of Materials

The following table comprises the most relevant third-party technologies used (general drivers not included).

| Vendor name / URL | Component name | Component version | Description / use |
|---|---|---|---|
| Accusoft | Pegasus PICTools Library | 2.0 | Image compression/decompression |
| Adobe Systems | Acrobat Reader | 11.0.17 | PDF Files reading |
| Boost.org | Boost | 1.46.1 | Image rendering |
| dicom.offis.de/dcmtk. | dcmtk | 3.6 | DICOM library |
| php.en | dcmtk | 4.5 | DICOM library |
| Dundas SW | Dundas Chart | 5.5 | UI library |
| GalaSoft | MVVM Toolkit | 4.0 | UI library |
| Intel | IPP | 6.1 | Signal processing |
| ijg.org | Libjpeg | 8.0 | Image compression/decompression |
| McAfee | Application Control | 7.0 | Whitelisting |
| Microsoft | Windows 7 | 7 Ultimate | Operating system |
| | .NET Framework | 3.5, 4.5, 4.6 | Programming framework |
| | Visual C++ Redistributable | 2008, 2010, 2012, 2013, 2015 | Programming framework |
| | Windows ADK | 10 | Deployment framework |
| | P&P Enterprise Library | 3.0 | Logging application |
| NVIDIA | CUDA runtime libraries | 8.0 | Runtime for CUDA code |
| | Control Panel | 375.63 | Video/Audio configuration software |
| Rogue Wave SW | Stingray Studio library | 11.1 | UI toolkit library |
| Siemens Healthineers | *syngo* Classic | VH22B | Siemens Healthineers |
| medical framework | TeamViewer | VA10B | Siemens Healthineers adaptation of TeamViewer |
| Siemens Healthineers | TeamViewer | VE10 | Siemens Healthineers |
| adaptation of TeamViewer | Glew | 1.6, 1.7 | OpenGL extensions |
| Siemens Healthineers | MNP | VI20C | Siemens Healthineers adaptation of HP Radia Notify |
| TomTec | StressEcho | 4.2 | Clinical apps |
| | Cardiac Calcs | 5.0 | Clinical apps |
| | VVI | 2.0 | Clinical apps |
| X-Rite | iProfiler | 1.7.1 | Monitor calibration |
| Vxl.sourforge.net | VXL | 1.15 | Signal processing libraries |

# Manufacturer Disclosure Statement According to IEC60601-1

Statement according to IEC 60601-1, 3rd Edition, Chapter 14.13

## 1. Network properties required by the system and resulting risks

1-1 The device is connected via Ethernet cable or wireless protocol to the hospital using a TCP/IP network with 1Gb/s.

- If the network is down, the network services (see below) are not available which can lead to the risks stated below.
- If the network is unavailable, medical images cannot be transferred for remote consultation.
- If the wireless network is incorrectly protected (for example, open Wi-Fi configuration), the attack surface of all the connected devices is much larger, which can lead to the risks stated below.
- If the recommended network performance (1Gbit/s) is not provided, the transfer of images is extended, and availability of images at destinations (e.g., for consulting) is delayed.
- Only the protocols shown in the table of used ports are needed for communication.

1-2 PACS system for archiving images/results

- If the PACS is not available:
  - images cannot be archived after the examination. In case of a system hardware failure, all non-archived images can be lost.
  - images cannot be archived after the examination. Examinations may no longer be possible because the hard drive is full as non-archived images cannot be automatically removed.
  - images cannot be archived after the examination. In case of manual deletion of images, unarchived images can be lost.
  - images are not available for remote consultation via PACS consoles.
  - prior images are not available.
- If the recommended network performance (1Gb) is not provided, the transfer time to PACS is extended, and the wait for switching off the system consecutive to the last transfer operations is prolonged.

1-3 DICOM printer

- If the DICOM printer is not available, film is not available for diagnosis/archive.

1-4 RIS system

- If the RIS system is not available:
  - the modality worklist is not available. This can lead to data inconsistencies as well as unavailability of images when sent to the PACS until they are manually coerced with the RIS data in the PACS.
  - In case of a Worklist Query time-out due to poor network transfer, there is a possibility that non-actual RIS data is used when registering a patient from the list of schedules on the system.

1-5 Network connection to the SRS server

- If the connection to the Smart Remote Services server is not available, then support from Siemens Healthineers service is limited.

1-6 Common medical protocol properties

- Protocols used in medical environments are typically unsecure, with the exception of Secure Smart Remote Services (using HTTPS).

## 2. Instructions for the responsible organization

2-1 Connection of the system to a network 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.

2-2 Subsequent changes to the network could introduce new RISKS and require additional analysis.

2-3 Changes to the network include:

- changes in network configuration
- connection to additional items to the network
- disconnecting items from the network
- update of equipment connected to the network
- upgrade of equipment connected to the network

2-4 The RESPONSIBLE ORGANIZATION is fully responsible for the security of the network to which the device is connected.

2-5 The RESPONSIBLE ORGANIZATION is fully responsible to ensure staff who have access to the device do not have the opportunity to provide any harm to the system.

2-6 The RESPONSIBLE ORGANIZATION has to ensure that the internal network cannot be accessed physically by non-authorized persons.

2-7 Staff of the RESPONSIBLE ORGANIZATION has to be trained in security. The RESPONSIBLE ORGANIZATION is responsible for providing this.

2-8 The RESPONSIBLE ORGANIZATION is fully responsible to ensure that only authorized medical/administrative staff shall have access to the device.

2-9 The RESPONSIBLE ORGANIZATION is fully responsible to ensure that visitors/patients do not have unsupervised physical access to the system.

2-10 The RESPONSIBLE ORGANIZATION shall provide access to the system for device administrators and device service engineers.

2-11 The RESPONSIBLE ORGANIZATION has at least one staff person with administrative rights who has access to the system.

2-12 The RESPONSIBLE ORGANIZATION shall ensure that neither access from the public internet or the organization's intranet to the device is possible.

2-13 The RESPONSIBLE ORGANIZATION is responsible to ensure physical security for the device.

2-14 The RESPONSIBLE ORGANIZATION shall ensure that access to services for the device from other equipment is possible only on a need-to-do basis. An adequate network topology with appropriate firewall settings shall be used.

2-15 The RESPONSIBLE ORGANIZATION is responsible for a secure infrastructure that makes it impossible to change, prevent, or tamper with data in transit in any way.

2-16 RECOMMENDATION: It is highly recommended that the RESPONSIBLE ORGANIZATION monitors the network for unusual traffic.

2-17 The RESPONSIBLE ORGANIZATION is responsible for the hard-drive encryption recovery keys, and it is to prevent the theft or loss of those keys.

## 3. Intended purpose of integrating the device into an IT network

3-1 To integrate the system into the clinical workflow, the whole ultrasound system will interact as a DICOM node in the clinical network.

3-2 The system is DICOM-compliant, allowing it to be connected to a network with other compliant devices for the exchange of images. Networking allows the 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.

3-3 The system connects to the network through an Ethernet cable or a wireless protocol. The network interfaces allow 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 for detailed viewing and long-term storage.

## 4. Risks and hazardous situations

4-1 **Unsuccessful data transfer not recognized**

Function: Archiving and Networking

Hazard: Wrong diagnosis / loss of acquisition data

Caution: Data transfers between systems are not verified automatically. Loss of data, if data is deleted locally before it has been successfully transferred to another system.

Measure: Since not all systems support automatic storage commitment, verify the correctness of the data transfer at the remote system before deleting the local data.

Effect on: Patient

4-2 **Incorrect or incomplete data transfer**

Function: Data Exchange – Network

Hazard: Wrong diagnosis, wrong examination / loss of acquisition data, loss of post processing results, corrupted data, inconsistent data

Cause: DICOM objects are sent/received/retrieved. While objects are being prepared or during transfer, not all DICOM objects that are not considered are deleted, corrupted or unintentionally manipulated. Data on the sender and receiver side is not consistent. Failure of transfer not recognized.

Measure: It has to be verified by testing, that there is no object loss during sending, which means:

- Verify that exception scenarios result in a failed job (and check for other exceptions in log files).
- Verify that error cases, which result in data not complying with the DICOM standard, are covered by exception scenarios.

Effect on: Patient

**4-3 Insecure or incorrectly configured clinical network**

Function: Network Security

Hazard: Incorrect diagnosis basis, wrong diagnosis, wrong treatment, delayed diagnosis, delayed therapy, wrong examination, repetition of examination / loss of acquisition data, corrupted data, system DoS

Caution: Unauthorized access may affect system performance and data security.

Cause: Any unauthorized access to the system may affect the system performance and data security and may lead to:

- Lowered system performance and/or non-operational system
- Loss of data security including loss of all patient data

Measure:

- Enable your system administrator to ensure network security and the security of the operational infrastructure
- Consult manuals for secure setup
- Perform system updates as required
- Run your medical device only in protected network environments, and do not connect it directly to public networks
- Set up firewalls
- Prevent configuration files from being changed by users
- Update and patch networked systems as required

Effect on: Patient, System

**4-4 Bitlocker recovery keys not available when needed**

Function: Hard drive encryption

Hazard: Loss of patient data, system DoS

Caution: Customer should keep Bitlocker recovery keys safe

Cause: If the customer opted for hard drive encryption, and if BitLocker fails to access the encrypted drive for whatever reason, then the recovery keys will be needed by Siemens Healthineers Service to pause encryption and have offline access to the hard drive and the patient data stored in it.

Effect on: Patient, System

## Manufacturer Disclosure Statement for Medical Device Security – MDS$^2$

### Device Description

| | | | |
|---|---|---|---|
| **Device Category**<br>Diagnostic Ultrasound | **Manufacturer**<br>Siemens Medical Solutions USA, Inc. | **Document ID**<br>(non-controlled document) | **Document**<br>Release Date<br>11/20/2017 |
| **Device Model**<br>S1000/S2000/S3000 | **Software Revision**<br>VE10 | **Software Release Date**<br>01/01/2017 | |
| Manufacturer or Representative Contact Information | **Company Name**<br>Siemens Medical Solutions USA, Inc. | **Manufacturer Contact Information**<br>Siemens Medical Solutions – Ultrasound<br>685 E Middlefield Rd, Mountain View, CA 94043 | |
| | **Representative Name/Position**<br>Ricardo Jimenez / Product Security Officer | | |

**Intended use of device in network-connected environment**

Optionally, the ACUSON S Family Ultrasound System can be configured to communicate to a hospital Patient Archival Communications System (PACS). The following DICOM services are supported: Store SCP / SCU, Modality Worklist SCU, Query / Retrieve SCU, Storage Commitment SCU, Print SCU and DICOM Structured Reporting SCU.
Optionally, the ACUSON S Family system can be configured to write a generated structured report to a Windows shared folder.
Optionally, the ACUSON S Family system can be configured to communicate with a Nuance PowerScribe® 360 | Reporting server to publish measurement results.

## Management of Private Data

| | | | | |
|---|---|---|---|---|
| Refer to Section 2.3.2 of HIMSS/NEMA HN 1-2013 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 | – |
| | B.5 | **Biometric data**? | Yes | 1 |
| | B.6 | Personal financial information? | No | – |
| **C** | | Maintaining **private data** – Can the **device**: | | |
| | C.1 | Maintain **private data** temporarily in volatile memory (e.g., until cleared by power-off or reset)? | Yes | – |
| | C.2 | Store **private data** permanently 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 dat**a 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 | – |
| | D.6 | Transmit/receive **private data** via an integrated wireless network connection (e.g., Wi-Fi, Bluetooth, infrared, etc.)? | Yes | – |
| | D.7 | Import **private data** via scanning? | Yes | – |
| | D.8 | Other? | N/A | – |
| Management of **private data** notes | | 1) The system can store height, weight and BSA. | | |

| | | | | |
|---|---|---|---|---|
| **Device Category**<br>Diagnostic Ultrasound | | **Manufacturer**<br>Siemens Medical Solutions USA, Inc. | **Document ID**<br>(non-controlled document) | **Document**<br>Release Date<br>11/20/2017 |
| **Device Model**<br>S1000/S2000/S3000 | **Software Revision**<br>VE10 | **Software Release Date**<br>01/01/2017 | | |

## Security capabilities

| | | | |
|---|---|---|---|
| Refer to Section 2.3.2 of HIMSS/NEMA HN 1-2013 standard for the proper interpretation of information requested in this form. | | Yes, No, N/A, or See Note | Note # |
| **1** | **Automatic logoff (ALOF)**<br>The **device’s** ability to prevent access and misuse by unauthorized **users** if the **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. The auto- logoff can be configured from 1 to 120 minutes. | | |
| **2** | **Audit controls (AUDT)**<br>The ability to reliably audit activity on the **device**. | | |
| 2-1 | Can the **medical device** create an **audit trail**? | Yes | – |
| 2-2 | Indicate which of the following events are recorded in the audit log: | | |
| 2-2.1 | Login/logout | Yes | – |
| 2-2.2 | Display/presentation of data | Yes | – |
| 2-2.3 | Creation/modification/deletion of data | Yes | – |
| 2-2.4 | Import/export of data from **removable media** | Yes | – |
| 2-2.5 | Receipt/transmission of data from/to external (e.g., network) connection | Yes | – |
| 2-2.51 | **Remote service** activity | Yes | – |
| 2-2.6 | Other events? (describe in the notes section) | No | – |
| 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: | Log items are encrypted as they are added to the audit log. | | |
| **3** | **Authorization (AUTH)**<br>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? | No | – |
| 3-2 | Can **users** be assigned different privilege levels within an application based on ‘roles’ (e.g., guests, regular **users**, power **users**, administrators, etc.)? | No | – |
| 3-3 | Can the **device** owner/**operato**r obtain unrestricted administrative privileges (e.g., access operating system or application via local root or admin account)? | No | – |
| AUTH notes: | | | |

| | | | | |
|---|---|---|---|---|
| **Device Category**<br>Diagnostic Ultrasound | | **Manufacturer**<br>Siemens Medical Solutions USA, Inc. | **Document ID**<br>(non-controlled document) | **Document**<br>Release Date<br>11/20/2017 |
| **Device Model**<br>S1000/S2000/S3000 | **Software Revision**<br>VE10 | **Software Release Date**<br>01/01/2017 | | |

| Refer to Section 2.3.2 of HIMSS/NEMA HN 1-2013 standard for the proper interpretation of information requested in this form. | | Yes, No, N/A, or See Note | Note # |
|---|---|---|---|
| **4** | **Configuration of security features (CNFS)**<br>The ability to configure/re-configure **device security capabilities** to meet **user's** needs. | | |
| 4-1 | Can the **device** owner/**operator** reconfigure product **security capabilities**? | No | – |
| CNFS notes: | 1. Reconfiguration of security features only through Siemens Healthineers Services representative. | | |
| **5** | **Cyber security product upgrades (CSUP)**<br>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? | Yes | 1 |
| 5-1.1 | Can security patches or other software be installed remotely? | Yes | 2 |
| CSUP notes: | 1. Only security patches that become available through Siemens Healthineers are subject to be installed in the system.<br>2. SRS can push patches to system, which are then installed once approved by the user. | | |
| **6** | **Health data DE-identification (DIDT)**<br>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 | 1 |
| DIDT notes: | 1. There is a feature in Patient Browser that will blank the patient banner and blank the DICOM tags identifying a particular patient. | | |
| **7** | **Data backup and disaster recovery (DTBK)**<br>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 (e.g., backup to remote storage or **removable media** such as tape, disk)? | Yes | 1 |
| DTBK notes: | 1. Patient data is uploaded to PACS during or after each exam. Patient Data can be backed up to USB or DVD. System configuration can be backed up to USB. | | |
| **8** | **Emergency access (EMRG)**<br>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. The system will allow for an emergency exam to be performed. Access to main aspects of the system other than that required to perform the exam are restricted. | | |
| **9** | **Health data integrity and authenticity (IGAU)**<br>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? | No | – |

| | | | | |
|---|---|---|---|---|
| **Device Category**<br>Diagnostic Ultrasound | | **Manufacturer**<br>Siemens Medical Solutions USA, Inc. | **Document ID**<br>(non-controlled document) | **Document**<br>Release Date<br>11/20/2017 |
| **Device Model**<br>S1000/S2000/S3000 | **Software Revision**<br>VE10 | **Software Release Date**<br>01/01/2017 | | |

| Refer to Section 2.3.2 of HIMSS/NEMA HN 1-2013 standard for the proper interpretation of information requested in this form. | | Yes, No, N/A, or See Note | Note # |
|---|---|---|---|
| **10** | **Malware detection/protection (MLDP)**<br>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 | – |
| 10-1.1 | Can the **user** independently re-configure **anti-malware** settings? | No | – |
| 10-1.2 | Does notification of **malware** detection occur in the **device user** interface? | N/A | 1 |
| 10-1.3 | Can only manufacturer-authorized persons repair systems when **malware** has been detected? | Yes | – |
| 10-2 | Can the **device** owner install or update **anti-virus software**? | No | 2 |
| 10-3 | Can the **device** owner/**operator** (technically/physically) update virus definitions on manufacturer-installed **antivirus software**? | N/A | – |
| MLDP notes: | 1. McAfee Application Control is incorporated into the system.<br>Only software signed by Siemens Healthineers can execute. | | |
| **11** | **Node authentication (NAUT)**<br>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. Communication to a PACS can be configured to use TLS certificates. Only if encrypted DICOM functionality is being used. | | |
| **12** | **Person authentication (PAUT)**<br>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 | – |
| 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 | – |
| 12-3 | Can the **device** be configured to lock out a **user** after a certain number of unsuccessful logon attempts? | No | – |
| 12-4 | Can default passwords be changed at/prior to installation? | Yes | – |
| 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 | – |
| 12-7 | Can the **device** be configured so that account passwords expire periodically? | No | – |
| PAUT notes: | | | |
| **13** | **Physical locks (PLOK)**<br>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 (e.g., cannot remove without tools)? | Yes | – |

| | | | | |
|---|---|---|---|---|
| **Device Category**<br>Diagnostic Ultrasound | | **Manufacturer**<br>Siemens Medical Solutions USA, Inc. | **Document ID**<br>(non-controlled document) | **Document**<br>Release Date<br>11/20/2017 |
| **Device Model**<br>S1000/S2000/S3000 | **Software Revision**<br>VE10 | **Software Release Date**<br>01/01/2017 | | |

| Refer to Section 2.3.2 of HIMSS/NEMA HN 1-2013 standard for the proper interpretation of information requested in this form. | | Yes, No, N/A, or See Note | Note # |
|---|---|---|---|
| **14** | **Roadmap for third-party components in the device life cycle (RDMP)**<br>Manufacturer's plans for security support of third-party components within the **device** 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). | Yes | 1 |
| 14-2 | Is a list available of other third-party applications provided by the manufacturer? | Yes | 2 |
| RDMP notes: | 1. Microsoft Windows 7 64-bit Operating System<br>2. See Software Bill of Materials | | |
| **15** | **System and application hardening (SAHD)**<br>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 | – |
| 15-3 | Does the device have external communication capability (e.g., network, modem, etc.)? | Yes | – |
| 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,** closed/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** (e.g., a source other than an internal drive or memory component)? | Yes | – |
| 15-11 | Can software or hardware not authorized by the device manufacturer be installed on the device without the use of tools? | Yes | – |
| SAHD notes: | 1. DISA STIGS | | |
| **16** | **Security guidance (SGUD)**<br>The availability of security guidance for the **operator** and administrator of the system and the manufacturer sales and service. | | |
| 16-1 | Are security-related features documented for the **device user**? | Yes | 1 |
| 16-2 | Are instructions available for **device**/media sanitization (e.g., instructions for how to achieve the permanent deletion of personal or other sensitive data)? | Yes | – |
| SGUD notes: | 1. The user manual has a security chapter for hardening the system. | | |

| | | | | |
|---|---|---|---|---|
| **Device Category**<br>Diagnostic Ultrasound | | **Manufacturer**<br>Siemens Medical Solutions USA, Inc. | **Document ID**<br>(non-controlled document) | **Document**<br>Release Date<br>11/20/2017 |
| **Device Model**<br>S1000/S2000/S3000 | **Software Revision**<br>VE10 | **Software Release Date**<br>01/01/2017 | | |

| Refer to Section 2.3.2 of HIMSS/NEMA HN 1-2013 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)**<br>The ability of the **device** to ensure unauthorized access does not compromise the integrity and confidentiality of private data stored on the **device** or **removable media**. | | |
| 17-1 | Can the **device** encrypt data at rest? | Yes | 1 |
| STCF notes: | 1. Microsoft BitLocker can be enabled at the factory or after customer installation. | | |
| **18** | **Transmission confidentiality (TXCF)**<br>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**?<br>(If yes, indicate in the notes which encryption standard is implemented.) | See Note | 1 |
| 18-3 | Is **private data** transmission restricted to a fixed list of network destinations? | Yes | – |
| TXCF notes: | 1. Encryption via industry standards is available with wireless networking. Application layer encryption is available only if encrypted DICOM functionality is being used. Secure DICOM can be configured to use TLS 1.0, 1.1, or 1.2. DICOM is encrypted using TLS_RSA_WITH_128_CBC_SHA or TLS_RSA_WITH_3DES_EDE_CBC_SHA. | | |
| **19** | **Transmission integrity (TXIG)**<br>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?<br>(If yes, describe in the notes section how this is achieved.) | Yes | 1 |
| TXIG notes: | 1. Industry standard data encryption, TLS protocol. Usage of these options enables transmission integrity and addresses man-in-the-middle scenarios. Secure DICOM uses TLS, which guarantees confidentiality and integrity of the data. | | |
| **20** | **Other security considerations (OTHR)**<br>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 user to accept or initiate remote access? | Yes | – |
| OTHR notes | | | |

# Abbreviations

| | |
|---|---|
| **AD** | Active Directory |
| **AES** | Advanced Encryption Standard |
| **BIOS** | Basic Input Output System |
| **DES** | Data Encryption Standard |
| **DICOM** | Digital Imaging and Communications in Medicine |
| **DISA** | Defense Information Systems Agency |
| **DMZ** | Demilitarized Zone |
| **DoS** | Denial of Service |
| **ePHI** | Electronic Protected Health Information |
| **FDA** | Food and Drug Administration |
| **FIPS** | Federal Information Processing Standards |
| **GPO** | Group Policy Object |
| **HHS** | Health and Human Services |
| **HIPAA** | Health Insurance Portability and Accountability Act |
| **HIMSS** | Healthcare Information and Management Systems Society |
| **HTTP** | Hypertext Transfer Protocol |
| **HTTPS** | HTTP Secure |
| **ICS** | Integrated Communication Services |
| **IEC** | International Electrotechnical Commission |
| **IVM** | Intervention Module |
| **LDAP** | Lightweight Directory Access Protocol |
| **MD5** | Message Digest 5 |
| **MDS$^2$** | Manufacturer Disclosure Statement |
| **MSTS** | Microsoft Terminal Server |
| **NEMA** | National Electrical Manufacturers Association |
| **NTP** | Network Time Protocol |
| **OCR** | Office for Civil Rights |
| **OU** | Organizational Unit |
| **PACS** | Picture Archiving and Communication System |
| **PHI** | Protected Health Information |
| **PII** | Personally Identifiable Information |
| **RIS** | Radiology Information System |
| **RPC** | Remote Procedure Call |
| **RSA** | Random Sequential Absorption |
| **SAM** | Security Accounts Manager |
| **SHA** | Secure Hash Algorithm |
| **SQL** | Structured Query Language |
| **SRS** | Smart Remote Services |
| **STIG** | Security Technical Implementation Guidelines |
| **SW** | Software |
| **TCP** | Transmission Control Protocol |
| **UltraVNC** | Ultra Virtual Network Computing |
| **UDP** | User Datagram Protocol |
| **VPN** | Virtual Private Network |

## Disclaimer According to IEC 80001-1

1-1 The Device has the capability to be connected to a medical IT network, which is managed under full responsibility of the operating legal entity (hereafter called "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.

1-2 This statement describes Device-specific IT networking safety and security capabilities. It is NOT a RESPONSIBILITY AGREEMENT according to IEC 80001-1:2010 / EN 80001-1:2011.

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

1-4 The RESPONSIBLE ORGANIZATION acknowledges that the Device's underlying standard computer with operating system is to some extent vulnerable to typical attacks such as malware or denial-of-service.

1-5 Unintended consequences (e.g., misuse/loss/corruption) of data not under control of the Device (e.g., after electronic communication from the Device to an IT network or to a storage media), 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

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

**Legal Manufacturer**
Siemens Medical Solutions USA, Inc.
Ultrasound
22010 S.E. 51st Street
Issaquah, WA 98029, USA
Phone: 1-888-826-9702
siemens-healthineers.com/ultrasound

*Published by Siemens Medical Solutions USA, Inc. · Order No. A91US-586-1C-4A01 · CIT13132 6909 0219 online · ©Siemens Medical Solutions USA, Inc., 2019*