



eHealth Solutions / Release VA40A / 2021-04-09 / Revision r66-g75a306e

# eHealth Solutions Product and Solution Security White Paper

# Contents

<b>1 Foreword</b>	<b>4</b>
1.1 The Siemens Healthineers Product and Solution Security Program . . . . .	4
1.2 Vulnerability and Incident Management . . . . .	4
1.3 Elements . . . . .	4
1.4 Contacting Siemens Healthineers about Product and Solution Security . . . . .	4
<b>2 Basic Information</b>	<b>5</b>
2.1 GDPR-EU Technical and Organizational Measures . . . . .	5
2.2 Operating Systems . . . . .	5
2.2.1 Client . . . . .	5
2.2.2 Browsers . . . . .	6
2.2.3 Mobile compability . . . . .	6
2.2.4 Server . . . . .	6
2.2.4.1 Operating System . . . . .	6
2.2.4.2 Database . . . . .	6
Oracle . . . . .	6
mongoDB . . . . .	6
2.2.5 Hypervisors . . . . .	6
2.3 Hardware Specifications . . . . .	6
2.4 Network Ports and Services . . . . .	7
2.5 User Account Information . . . . .	7
2.6 Patching Strategy . . . . .	8
2.7 Cryptography Usage . . . . .	8
2.8 Handling of Sensitive Data (Transmission and Storage) . . . . .	8
2.9 Data Recovery . . . . .	9
2.10 Boundary Defense . . . . .	9
2.11 Terms and Conditions . . . . .	10
<b>3 Network Information</b>	<b>11</b>
3.1 eHealth HL7 FHIR Services . . . . .	11
<b>4 Security Controls</b>	<b>12</b>
4.1 Malware Protection . . . . .	12
4.2 Web Application Firewalls . . . . .	12
4.3 Controlled Use of Administrative Privileges . . . . .	12
4.4 Authentication and Authorization Controls . . . . .	12
4.4.1 Authentication . . . . .	12
4.4.2 Authorization . . . . .	13
4.5 Continuous Vulnerability Assessment and Remediation . . . . .	14
4.6 Security Scanning . . . . .	14
4.7 Hardening . . . . .	17
4.8 Network Controls . . . . .	18
4.9 Physical Safeguards . . . . .	18
4.10 Data Protection Controls . . . . .	18
4.11 Encryption . . . . .	18
4.11.1 File-System Encryption . . . . .	18
4.11.2 Document Encryption . . . . .	18
4.12 Auditing/Logging . . . . .	19
4.13 Remote Connectivity . . . . .	19
4.14 Administrative Controls . . . . .	19

4.15 Incident Response Management . . . . .	19
<b>5 Shared Responsibilities</b>	<b>20</b>
<b>6 Software Bill of Materials</b>	<b>21</b>
<b>7 Manufacturer Disclosure Statement (MDS2)</b>	<b>22</b>
<b>8 Abbreviations</b>	<b>29</b>
8.1 Disclaimer According to IEC 80001-1 . . . . .	29
8.2 Statement on FDA Cybersecurity Guidance . . . . .	30

# 1 Foreword

## 1.1 The Siemens Healthineers Product and Solution Security Program

At Siemens Healthineers, we are committed to working with you to address cybersecurity and privacy requirements. Our Product and Solution Security Office is responsible for our global program that focuses on addressing cybersecurity throughout the product lifecycle of our products. Our program targets incorporating state of the art cybersecurity in our current and future products. We seek to protect the security of your data while, at the same time, providing measures to strengthen the resiliency of our products from external cybersecurity attackers. We comply with applicable 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 you meet your IT security and privacy obligations.

## 1.2 Vulnerability and Incident Management

Siemens Healthineers cooperates with government agencies and cybersecurity researchers concerning reported potential vulnerabilities. Our communications policy strives for coordinated disclosure. We work in this way with our customers and other parties, when appropriate, in response to potential vulnerabilities and incidents in our medical devices, no matter what the source.

## 1.3 Elements

The Elements of our product and solution security program are:

- Providing information to facilitate secure configuration and use of our medical devices in your IT environment
- Conducting formal threat and risk analysis for our medical devices
- Incorporating secure architecture, design and coding methodologies in our software development process
- Performing static code analysis of medical device software
- Conducting security testing of medical devices under development as well as medical devices already in the field
- Tailoring patch management to the medical device and depth of coverage chosen by you
- Monitoring security vulnerability to track reported third party components issues in our medical devices
- Working with suppliers to address security throughout the supply chain
- Training of employees to provide knowledge consistent with their level of responsibilities regarding your data and device integrity.

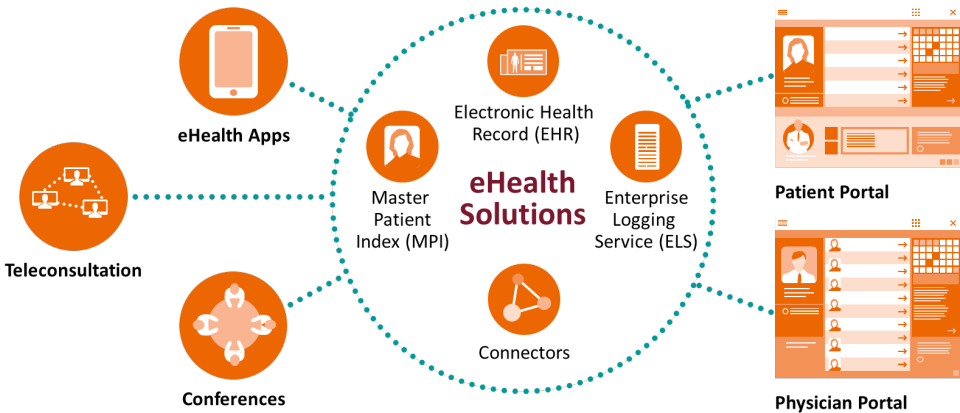
## 1.4 Contacting Siemens Healthineers about Product and Solution Security

Siemens Healthineers requests that any cybersecurity or privacy incidents are reported by email to: <mailto:productsecurity@siemens-healthineers.com>

For all other communication with Siemens Healthineers about product and solution security: [ProductTechnologyAssurance.dl@siemens-healthineers.com](mailto:ProductTechnologyAssurance.dl@siemens-healthineers.com)

# 2 Basic Information

Figure 1: Overview of eHealth Solutions services and applications



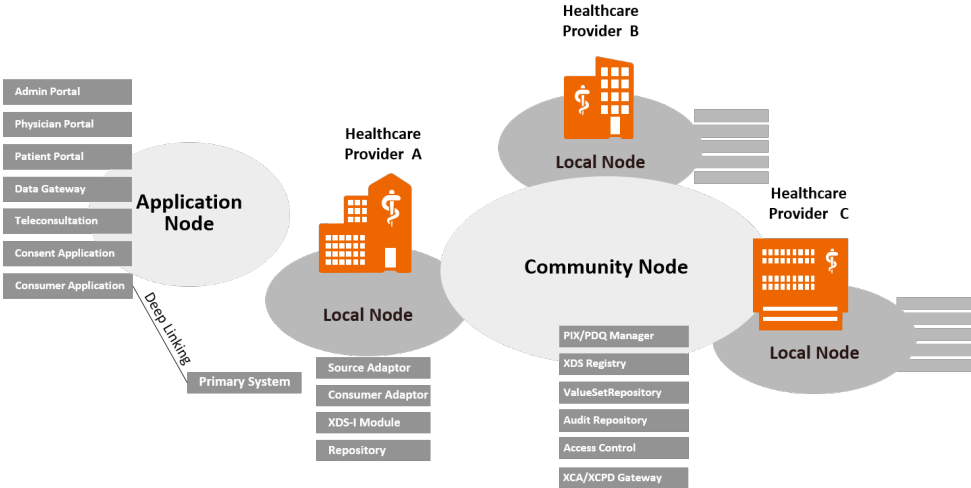
eHealth Solutions connects institutions for cooperative care and optimized communication.

A high level of data security and patient safety is a key success factor for end user acceptance and trust in electronic health records.

## 2.1 GDPR-EU Technical and Organizational Measures

Technical and Organizational Measures (TOMs) required for compliance with the EU General Data Protection Regulation 2016/679 (GDPR) are addressed in the following sections.

Figure 2: Component View of eHealth Solutions Services



## 2.2 Operating Systems

### 2.2.1 Client

There are no special operating system requirements for clients.

## 2.2.2 Browsers

Web applications can be accessed with current web browser software. All operating systems that have HTML5- and JavaScript-enabled browsers are supported. On Windows, the following browsers are supported:

- Google Chrome ≥ 85 (recommended)
- Mozilla Firefox ≥ 81 (supported)
- Microsoft Edge ≥ 85 (supported)
- Microsoft Internet Explorer ≥ 11 (supported, except Virtual Visits application)  
Performance issues, e.g. drop-down menus.
- Safari ≥ 12 (supported)

## 2.2.3 Mobile compability

On Apple OS X with Safari and mobile operating systems like Android, Apple iOS, and Microsoft Windows 10, web applications are supported but not optimized for touch gestures.

## 2.2.4 Server

### 2.2.4.1 Operating System

- Red Hat Enterprise Linux 7.6–7.8

### 2.2.4.2 Database

#### Oracle

- Oracle 11.2.0.4: for legacy upgrades only
- Oracle 12.2.0.1: supported
- Oracle 19.3: recommended for new Installations

#### mongoDB

- 4.2

## 2.2.5 Hypervisors

eHealth Solutions can be deployed in a virtualization environment. The following hypervisors are supported:

- VMware vSphere ≥ 6.5 (recommended)
- any certified Hypervisor for Red Hat Enterprise Linux 7.6 (supported — please refer to official Red Hat Documentation)

## 2.3 Hardware Specifications

### Client

There are no special hardware requirements for clients.

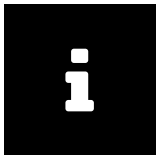
## Server

There are no special hardware requirements for server machines because eHealth Solutions is operated as virtual machines. Specification of virtual RAM (vRAM) and virtual (vCPU) depends on the expected load (volume of documents, patients, concurrent access).

For the deployment of eHealth Solutions (= smallest possible deployment, incl. 1 Configuration Node, 1 Community Node, 1 Local Node, 1 Application Node), the following minimal VM size is recommended for testing and demo environments.

**Table 1:** Virtual Hardware Requirements

Attribute	Sizing pre-configured eHealth Solutions VM Container
vCPU	6 cores
vRAM	32 GB
Disk	360 GB
Storage/Repository	50 GB
Network Bandwidth	100 MBit



### Note

- The actual configuration of hardware and software components may vary from customer to customer depending on the final solution design.
- For increased performance and protection, it is recommended to use RAID configuration with write cache enabled.
- The dimensions needed for database storage are calculated separately depending on the data and transaction volume of the installation.

## 2.4 Network Ports and Services

eHealth Solutions uses the following network services:

- Web application (HTTPS)
- Web services (SOAP over HTTPS)
- Web sockets (WSS)
- HL7 (TCP and TLS)
- DICOM (TCP and TLS)
- (Secure) Network Time Protocol – NTP (UDP)
- SSH (TCP)
- Syslog over TLS (TCP)

For details, see the network diagram and the network requirements ([Section 3](#)).

## 2.5 User Account Information

The following types of users exist:

- Patients
- Healthcare professionals

- Administrative staff for clearing operations, etc.

## 2.6 Patching Strategy

General descriptions of application updates are provided in the Administration Manual. Project-specific maintenance intervals and update strategies have to be defined and followed to ensure that the most current environment is installed.

A complete list of third-party software and libraries is included in the Release Notes of the product.

## 2.7 Cryptography Usage

- Beside authorization and access control, eHealth Solutions uses symmetric as well as asymmetric cryptography to prevent clinical data from being exposed to unauthorized persons.
- Cryptography to be used for healthcare systems is defined by the IHE Integration Profile Audit Trail and Node Authentication (ATNA).
- The ATNA profile requires TLS encryption for any clinical data submitted via network link.
- Minimum key length and allowed cryptographic algorithms and protocols are defined by the ATNA profile.
- Application Server configuration only accepts ciphers and protocols with highest security rating.

## 2.8 Handling of Sensitive Data (Transmission and Storage)

- Electronic Protected Health Information (ePHI)
- Personally Identifiable Information (PII)

Patient and clinical data are defined as particularly sensitive according to European and international legislation. Thus, Siemens Healthineers eHealth Solutions ensures continuous product and solution security as well as patient safety throughout the entire software and deployment life cycle. Secure coding instructions are directly incorporated in the software development guidelines.

By design, persistence of and access to patient and clinical data are limited by appropriate service-oriented architecture. The eHealth Solutions architecture relies on the IHE Cross-Enterprise Document Sharing (XDS) Integration Profile. The architectural design thus strictly separates patient demographic data from clinical data by using dedicated services whose interfaces are subject to authorization and access control measures. Configuration options are available to prevent any service other than the Master Patient Index and the Document Repository from persisting demographic patient data. This allows strict physical separation of personally Identifiable Information (PII) and Electronic Protected Health Information (ePHI) e.g. by using different provider or data centers.

Country-specific legislation and organizational requirements are accommodated by flexible security configuration such as authentication and role- and context-based access control. Individual measures for deployment and operation ensure the highest possible level of privacy in the exchange of personal health-related data.

The following table lists services that persist and process Personally Identifiable Information (PII) and Electronic Protected Health Information (ePHI):



**Table 2**

Service/Component	Type of Information	Persistence Details
Document Repository	ePHI	Clinical documents
Image Management Module	ePHI	ePHI as DICOM image data in image cache
Document Registry	PII, (ePHI)	Metadata with pseudonymized PI; partially ePHI such as institution or department of treatment
National Service Gateway	PII, ePHI	Cached ePHI such as clinical documents, depending on national requirements
Master Patient Index (PIX)	PII	Patient demographic data, e.g. name, address, date of birth, sex
Audit Record Repository	PII	ATNA Audit logs containing pseudonymized PII
Healthcare Provider Directory	PII	Healthcare professional data
Access Control System	PII	Access control policies containing pseudonymized PII
Technical Logs	PII	Master Patient Index log files contain patient demographic data of submitted source patients. Additional log files persisted in the configured log file path may contain PII.
Health Data Repository	PII, ePHI	Forms may contain PII and ePHI.
Observation Service	PII, ePHI	Medical data with pseudonymized ePHI is persisted as coded values by the Observation Service. Processed data emerges from documents or other data sources.

Services not listed in the table above either do not persist PII or PHI at all or in a pseudonymized manner. In the latter case only identifiers are persisted. Resolving identifiers requires invocation of distributed services which are subject to access control and audit logging.

## 2.9 Data Recovery

Data and machine recovery strategies should be implemented by operator. This includes disaster recovery mechanisms and offline backups. Particular measures have to be taken by operator to prevent data loss e.g. in case of crypto malware spreading in operator's networks.

Recovery mechanisms should be implemented according to customer-specific guidelines.

Detailed instructions for Backup of nodes and databases can be found in the eHealth Solutions Installation and Operation Manual.

## 2.10 Boundary Defense

Common boundary defense measures should be implemented by operator. The following measures should be taken in accordance to customer-specific guidelines:

- Network separation using Firewalls and Demilitarized Zones (DMZs)
- Reverse Proxy and Web Application Firewall upstream of Portal Applications
- Intrusion Prevention Systems
- Malware protection with site-specific anti-malware solution
- Site-specific physical access controls

Specific configuration instructions for above-mentioned boundary defense measures are described where applicable in administrative manuals.

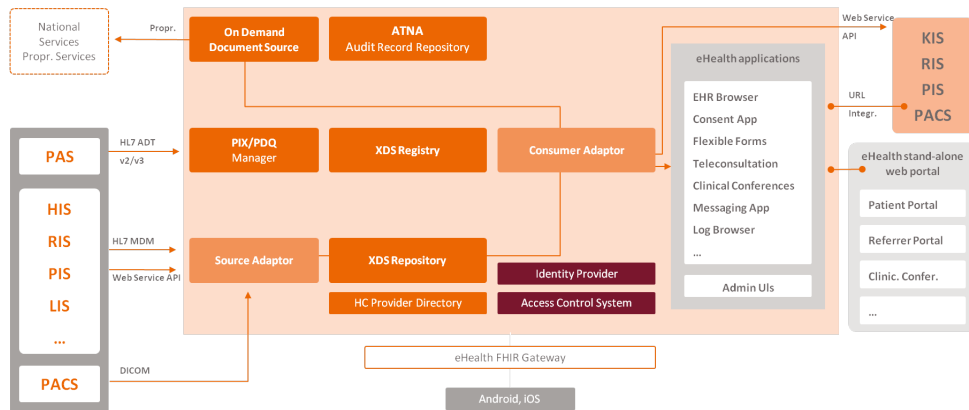
## **2.11 Terms and Conditions**

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

# 3 Network Information

The following table lists default TCP and UDP network ports for productive environments. Testing and pre-productive environments may use additional unencrypted ports. Port numbers are configurable and may vary according to customer settings.

**Figure 3:** Network Connections Including Internal Communication and Connectivity with Primary Systems



**Table 3**

Port number	Service/Function	Direction	Protocol
22	Management access via SSH	Inbound	TCP
123	Network time protocol and secure network time protocol for time synchronization	Bidirectional	UDP
443, 8443	Web applications for physicians, patients, admins	Inbound	HTTPS, HL7 FHIR
5232	Audit messages for IHE ATNA logging	Inbound	TCP (Syslog over TLS)
5239	HL7 MDM stream for document management	Inbound	HL7 over TLS
5240	HL7 ADT stream for patient management	Inbound	HL7 over TLS
11113, 11114	DICOM image registration	Inbound	DICOM over TLS
443, 6443, 7443, 9443	Web services for Consumer, Source, Configuration, Registry, Repository and Gateways	Bidirectional	HTTPS

## 3.1 eHealth HL7 FHIR Services

RESTful service interfaces are exposed by eHealth Solutions to facilitate interaction with mobile and web-based applications. The eHealth Solutions Data Gateway serves as single point of contact for mobile applications connecting to the eHealth Solutions infrastructure. Restful service interfaces provided by the Data Gateway are compliant to the HL7 Fast Healthcare Interoperability Resources (FHIR) specification. Detailed interface descriptions are available in the HL7 Conformance Statement.

Exposed RESTful FHIR services rely on the below-mentioned HTTPS communication including ciphers and protocols with highest security rating. Authentication, Authorization and Access Control is handled via JSON Web Token (JWT) compliant to IHE Internet User Authorization (IUA) as described in [Section 4.4](#).

# 4 Security Controls

## 4.1 Malware Protection

- Server-side malware protection as well as intrusion detection and prevention systems are supported by the product.
- The operator is responsible for the integration of the product in site-specific malware protection environments.

Content validation and virus scanning can be activated at two distinct entry points:

1. before document submission to repository
2. before document download via document consumer

Content validation ahead of the repository prevents undesired and potentially malicious content to be registered at repositories. Content validation before download prevents malware to reach client systems in case remote Repositories are not covered by scans with recent malware signatures.

## 4.2 Web Application Firewalls

A Web Application Firewall (WAF) should be deployed ahead of eHealth Solutions portal applications. Common web application attacks are prevented by WAFs before they reach the portal applications.

It is the responsibility of the operator to set up and deploy a site-specific Web Application Firewall. Recommendations for WAF configuration is provided in the Administrator Manual.

## 4.3 Controlled Use of Administrative Privileges

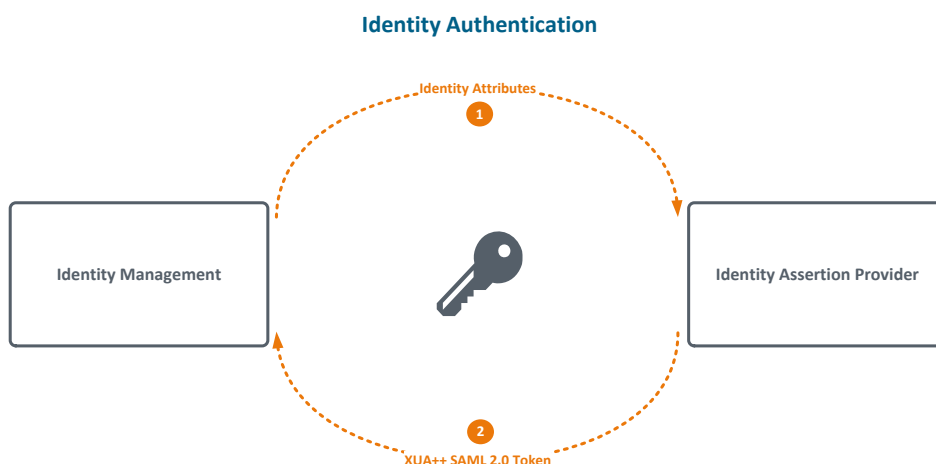
- The system distinguishes between clinical and administrative roles.
- Clinical users do not require administrative privileges. Authorization as administrator is required for administrative tasks.
- Fine-grained privileges for administrative subtasks can be configured.
- Administrative interactions as well as configuration changes are subject to audit logging.

## 4.4 Authentication and Authorization Controls

### 4.4.1 Authentication

- User authentication and role information are handled by a security Assertion Markup Language (SAML) 2.0- and IHE XUA (Cross-Enterprise User Assertion)-compliant Identity Provider (IdP).
- User and role information is submitted from a trusted primary system (e.g. HIS, CIS) authenticated by client certificates.
- Manual user management via portal applications.
- Automatic user management by connecting existing user directories, e.g. LDAP.

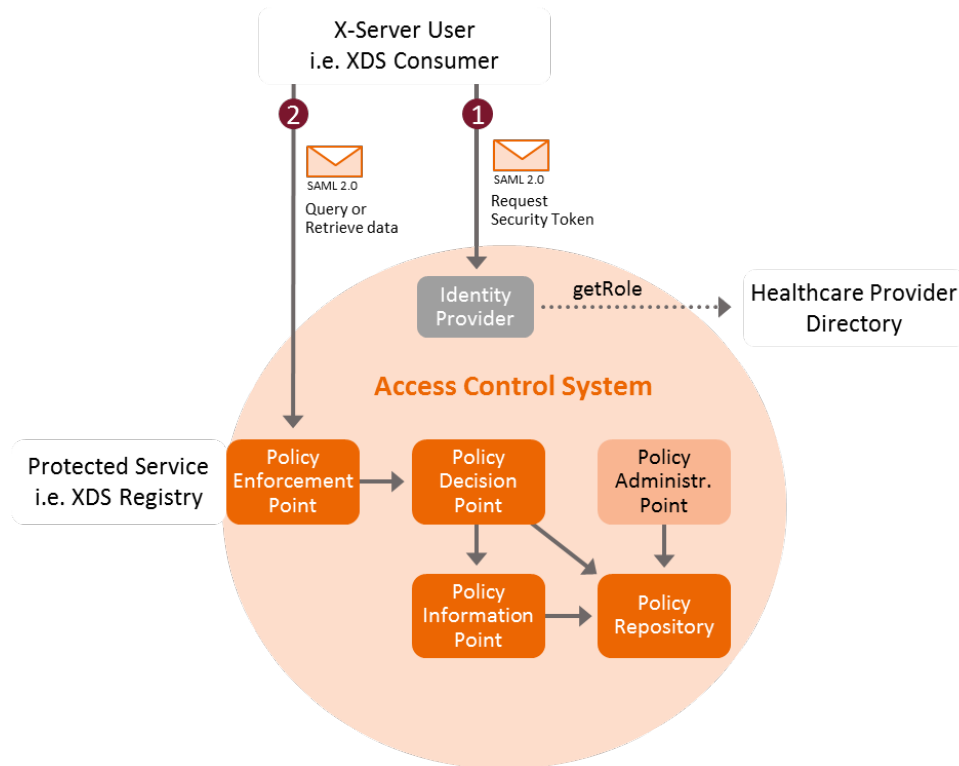
Figure 4: Authentication via Built-in or External Identity Provider



#### 4.4.2 Authorization

- User authorization is based on eXtensible Access Control Markup Language (XACML) policies that offer a state-of-the-art role- and context-based access control system compliant to IHE Advanced Patient Privacy Consents (APPC).
- The general behavior of the access control system can be pre-configured via policies to reflect current legal and organizational requirements, e.g. opt-in vs. opt-out configuration.
- Patient consent declarations are also persisted as policies.
- Role and context information (e.g. emergency access) transmitted in the SAML token is evaluated by the access control system.
- User Identity, Attributes, and Authorizations for RESTful services is supported by JSON Web Token (JWT) compliant to IHE Internet User Authorization (IUA)

**Figure 5:** eHealth Solutions Access Control System Including Authentication via SAML Identity Provider



#### 4.5 Continuous Vulnerability Assessment and Remediation

Continuous vulnerability assessment and remediation is performed throughout the entire product life cycle. The processes of software development, quality management and change management are certified according to EN ISO 13485 and EN ISO 9001 and comply to EU Council Directive 93/42/EE. Risk analysis and the identification of control measures are carried out with a particular focus on data security and patient safety. Upcoming and changed customer and market requirements as well as software anomalies (Bugs) are thoroughly evaluated in the risk management process according to *EN ISO 14971 Medical devices - Application of risk management to medical devices*. This process encompasses the identification, analysis and evaluation of risks as well as the deduction of control measures including monitoring of their realization.

The legal manufacturer, the Siemens Healthineers company ITH icoserve, is certified according to the strict criteria of EuroREC (<http://www.eurorec.org>) for usability and privacy for electronic health records.

Continuous vulnerability monitoring of third party components such as software libraries or application servers is implemented according to Siemens Healthineers Policies.

#### 4.6 Security Scanning

Periodic internal penetration testing provides for robustness against known vulnerabilities and attack patterns. eHealth Solutions has been subjected to an intensive security analysis carried out by the Department of Computer Science of the Leopold Franzens University of Innsbruck, which is a leading research facility in the field of software quality and data security. Penetration testing against commonly known vulnerabilities, including the OWASP Top 10 (see Section 4.6), was subject of this security analysis, as well

as an evaluation of the entire development process. This report provides evidence of a secure software development process that leads to products which fulfill the highest security requirements.

Penetration tests of the entire solution deployed at customers' sites have been carried out directly before go-live by XSEC infosec GmbH (<https://www.xsec.at/en/>), which focuses on security auditing and consulting.

The software and the entire solution have been subjected to security audits carried out in the scope of the Austrian Electronic Health Record (ELGA).

Portal applications are based on a widely used and well-tested Enterprise Portal Solution. The Enterprise Portal Solution follows the Open Web Application Security Project OWASP Top 10 and CWE/SANS Top 25 lists to ensure the highest possible security. Following these recommendations offers protection against known kinds of attacks and security vulnerabilities. Portal applications running on Enterprise Portal directly benefit from these commitments and can therefore be considered highly robust against the OWASP Top 10 security flaws. Additionally, eHealth Solutions web applications are developed with an awareness of the OWASP Top 10 security issues, as well as further security patterns. The constant training of the developers with a particular focus on those patterns ensures the development of eHealth Solutions web applications that provide robust designs against the OWASP Top 10 criteria. Periodic penetration testing of the software by independent organizations (see above) is an effective measure to prove the software's stability and vigilance.

The legal manufacturer, Siemens Healthineers company ITH icoserve, actively participates in the Siemens Product and Solution Security Initiative to ensure that cutting-edge security measures are employed and upcoming risks are identified and mitigated instantly.

An information security management system (ISMS) is employed to ensure that threats and vulnerabilities of third-party products, such as virtualization environments, operating systems, databases and software libraries, are constantly monitored using reliable sources such as CERT ([www.cert.at](http://www.cert.at)) for general advisories and Siemens CERT (<https://www.siemens.com/cert>) for specific advisories.

The development process follows the requirements of the IEC 62304, IEC 82304 and EN ISO 14971 including mandatory coding style guidelines. The application of state of the art version control systems provides access control and auditing for source code modifications, thus ensuring that source code can only be maintained by authorized developers. Robustness against the OWASP Top 10 criteria is achieved as follows:

**Table 4**

Criterion	Description
A1:2017 Injection	<ul style="list-style-type: none"> <li>➤ Covered by the security mechanism of the portal application.</li> <li>➤ Additionally: Input validation and usage of parametrized stored queries for the object-relational data mapper.</li> <li>➤ External Security Audits have placed special emphasis on robustness against injection attacks.</li> </ul>

Table 4: 

Criterion	Description
A2:2017 <b>Broken Authentication and Session Management</b>	Covered by the security mechanism of the portal application by usage of configurable, well-established authentication mechanisms such as: <ul style="list-style-type: none"> <li>➤ LDAP</li> <li>➤ Active Directory</li> <li>➤ OpenSSO</li> <li>➤ OpenID</li> <li>➤ SAML 2.0</li> <li>➤ Generation and persistence of user credentials via strong cryptography</li> <li>➤ Multi-factor authentication and Single-Sign-On compliant with IHE XUA</li> </ul>
A3:2017 <b>Sensitive Data Exposure</b>	<ul style="list-style-type: none"> <li>➤ Covered by the security mechanism of the portal application by usage of strong cryptography for transport encryption (TLS 1.2) and persistence of user credentials.</li> <li>➤ Transport encryption compliant with IHE ATNA requiring secure algorithms and high key length.</li> </ul>
A4:2017 <b>XML External Entity (XXE)</b>	XXE protection is provided by: <ul style="list-style-type: none"> <li>➤ Server-side stylesheet rendering and input validation.</li> <li>➤ Continuous checks of XML documents such as CDA documents or stylesheets against schemata.</li> </ul>
A5:2017 <b>Broken Access Control</b>	<ul style="list-style-type: none"> <li>➤ XACML-compliant Access Control System with flexible configuration of policies to reflect patient consent declarations.</li> <li>➤ Compliant with IHE Access Control Requirements.</li> <li>➤ Covered by the security mechanism of the portal application as well as by role- and context-based authorization.</li> </ul>
A6:2017 <b>Security Mis-configuration</b>	<ul style="list-style-type: none"> <li>➤ Covered by the security mechanism of the portal application by usage of well-established architectural design (security by design) for separation of components.</li> <li>➤ Usage of most recent versions and security patches.</li> <li>➤ Checklists for productive installations which comprise:               <ul style="list-style-type: none"> <li>➤ Installation of no other than required packages</li> <li>➤ Deactivation of unused ports</li> <li>➤ Solely encrypted communication</li> </ul> </li> <li>➤ Observance of customer-specific requirements concerning authentication policies (password length and complexity, Single Sign-On, multifactor authentication).</li> </ul>
A7:2017 <b>Cross-Site Scripting (XSS)</b>	<ul style="list-style-type: none"> <li>➤ Covered by the security mechanism of the portal application by input validation and additionally consequent escaping of output content.</li> <li>➤ External Security Audits have placed special emphasis on robustness against XSS attacks.</li> </ul>



Criterion	Description
A8:2017 <b>Insecure Deserialization</b>	Usage of well-established XML bindings as well as strict type checks against XMS schemata.
A9:2017 <b>Using Components with Known Vulnerabilities</b>	<ul style="list-style-type: none"> <li>➤ Continuous monitoring and reaction to known vulnerabilities.</li> <li>➤ Continuous monitoring of vulnerability lists.</li> <li>➤ Web-based management interfaces allow easy-to-use update with minimal downtime.</li> </ul>
A10:2017 <b>Insufficient Logging &amp; Monitoring</b>	<ul style="list-style-type: none"> <li>➤ Audit Logging complaint to IHE ATNA Secure Node Requirements.</li> <li>➤ Detailed, distributed technical logs.</li> <li>➤ Web-based reports from the ATNA Audit Record Repository.</li> <li>➤ Optional integration of fraud-detection mechanisms.</li> <li>➤ Secure time synchronization compliant with IHE CT Secure Time Client/ Server.</li> </ul>

## 4.7 Hardening

The following operating system- and application-specific hardening measures are recommended:

- Removal of unnecessary packages is handled by the default installation of the operating system.
- Secure Shell (SSH) access only by public-key authentication: Configured and activated by the operator.
- Setup and validation of a Secure Time Server (SNTP).
- Use of reverse proxies for accessing web applications from untrusted networks: Provided by default setup where applicable. Additional reverse proxies may be deployed by the operator.
- Adaptation of site-specific firewalling rules so that connections are restricted to the required ports of the applications. See above. Handled by the operator.
- Installation and deployment of network intrusion prevention systems and malware protection.
- Deactivation of unused services and eHealth Solutions applications: Handled by the application configuration.
- Activation of encryption-only communication paths: Handled by the application configuration.
- Application of customer-specific password complexity and validity rules for application and OS passwords.

Operating System specific hardening measures according to the Security Technical Implementation Guides (STIGs) standardized hardening measures.

It is the responsibility of the operator to set up and implement the operating system hardening. Recommendations for STIGs criteria to be applied are available in the Administrator Manual.

On productive and pre-productive environments, a post-installation security checklist is processed to ensure that the above-mentioned hardening measures have been sufficiently implemented.

## 4.8 Network Controls

- The system is designed to make limited use of network ports and protocols.
- Portal applications should be deployed in dedicated Demilitarized Zones (DMZs) separated from internet as well as from internal networks.
- A Reverse Proxy should be deployed upstream of Portal applications. Reverse Proxy may be combined with Web Application Firewall as described above

Detailed deployment recommendations for DMZs and reverse proxy are available in the Administrator Manual.

## 4.9 Physical Safeguards

The customer is responsible for the physical protection of the server infrastructure, e.g. by providing a safe server rack or a server room with access control.

## 4.10 Data Protection Controls

- PII as well as ePHI is protected by role-based access control.
- The system provides auditing of ePHI access.
- Confidentiality and integrity of ePHI/PII transmitted via networks is protected by strong cryptography between the client and the service.
- The system follows the strict requirements of the IHE Integration Profile Audit Trail and Node Authentication ATNA.
- Client and service certificates are required for service authentication and transport encryption.

## 4.11 Encryption

eHealth Solutions offers two encryption possibilities: one on file-system level, one on document level.

### 4.11.1 File-System Encryption

- The vendor encourages customers to use storage and database encryption. Encryption must be enabled by the customer and requires appropriate licensing of the Oracle database.
- A detailed backup and recovery concept is discussed with the customer for site-specific operations.

End2End content encryption allows documents to be persisted in an encrypted form in the XDS Document Repository. The Repository uses asymmetric encryption to encrypt the document for a specific client (Consumer). The corresponding certificate is provided by the consumer. In combination with document routing this asymmetric encryption allows documents to be decrypted solely by a specific consumer.

### 4.11.2 Document Encryption

To ensure secure data storage on document level, eHealth Solutions uses the encryption algorithm AES /GCM/NoPadding and the HashiCorp Vault.

- The unencrypted file is stored in a temporary storage where it will be deleted right after encryption.

- All plaintext keys are only kept in main memory (as short as possible), are not stored anywhere else and are immediately deleted after en- or decryption.
- For security reasons, the keys are only valid for one single document. This method is designed to prevent malicious intentions of gaining inappropriate access to documents. Should a heapdump be able to extract a key from main memory, only the document assigned to this key can be decrypted.
- As memory overflow could happen, a limit for the file size can be set in the Repository configuration.

#### **4.12 Auditing/Logging**

HIPAA- and IHE ATNA-compliant auditing of operations on ePHI, PII and user information such as:

- Login/logout
- Read access to ePHI (e.g. patient identification, document search and retrieval)
- Write access (provision, modification, deletion of ePHI)
- Administrative operations (e.g. clearing)
- Configuration changes

#### **4.13 Remote Connectivity**

- Siemens Remote Service connection is established using a secure channel. The channel is used e.g. to download security patches and updates.
- Operating system patches can be directly retrieved from the OS vendor or from a software repository operated by the manufacturer via Internet connection.
- Management of the operating system configuration is performed via Secure Shell (SSH) access.

#### **4.14 Administrative Controls**

- Administrative operations are strictly bound to named users.
- Usage of external authentication services (LDAP) is supported.
- Administrative interactions are subject to access control and audit logging.
- Fine-grained administrative permissions allow the limitation of access to ePHI by administrative staff.

#### **4.15 Incident Response Management**

The Siemens CERT Incident Response Process is used to react to incidents.

## 5 Shared Responsibilities

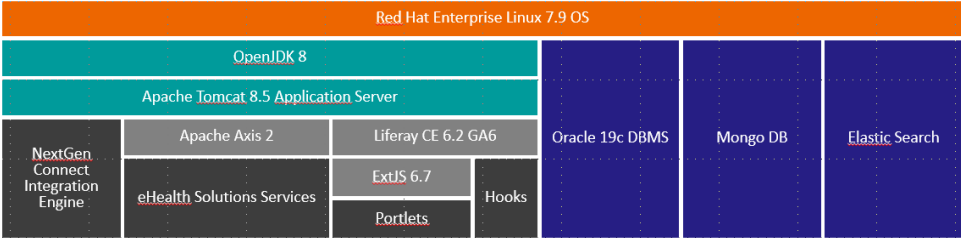
eHealth Solutions is designed and pre-configured following the security and privacy per design and per default approach. Deployment of eHealth Solutions in customer data centers entails the following site-specific responsibilities for the operator:

- Physical security and access control
- Maintenance and continuous upgrade of operating system as agreed on in maintenance contracts
- Backup and data recovery mechanisms as described above
- Implementation of site-specific boundary defense mechanisms such as firewalls and malware prevention as described above.

# 6 Software Bill of Materials

eHealth Solutions uses, among others, the following third-party software:

**Figure 6:** Third-party software in eHealth Solutions.



A complete list of third-party software and libraries is included in the product Release Notes.

## **7 Manufacturer Disclosure Statement (MDS2)**

**Manufacturer Disclosure Statement for Medical Device Security -- MDS2**

ITH icoserve Ges.m.b.H eHealth Solutions VA388

MDS2\_eHealth\_VA388\_v1.0

23.11.2020

Question ID	Question	See note	IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
DOC-1	Manufacturer Name	ITH icoserve Ges.m.b.H	---		
DOC-2	Device Description	eHealth Solutions	---		
DOC-3	Device Model	eHealth Solutions VA378	---		
DOC-4	Document ID	MDS2_eHealth_VA378_v1.0	---		
DOC-5	Manufacturer Contact Information	ITH icoserve technology for healthcare GmbH A Siemens Healthineers Company Innrain 98 6020 Innsbruck Austria Tel: +43512890590 Email: <a href="mailto:office@ith.icoserve.com">office@ith.icoserve.com</a>	---		
DOC-6	Intended use of device in network-connected environment:	eHealth Solutions is a networking solution for the digital management of services in the healthcare sector. eHealth Solutions is able to protect uploaded patient data against unauthorized access in a multitude of ways via a customizable and finely controllable access control system.	Full description contained in user manuals.		
DOC-7	Document Release Date	16.01.2020	---		
DOC-8	Coordinated Vulnerability Disclosure: Does the manufacturer have a vulnerability disclosure program for this device?	Yes	Siemens Healthineers Vulnerability disclosure process is applied.		
DOC-9	ISAO: Is the manufacturer part of an Information Sharing and Analysis Organization?	Yes	---		
DOC-10	Diagram: Is a network or data flow diagram available that indicates connections to other system components or expected external resources?	Yes	See Product and Solution Security Whitepaper		
DOC-11	SaMD: Is the device Software as a Medical Device (i.e. software-only, no hardware)?	Yes	---		
DOC-11.1	Does the SaMD contain an operating system?	Yes	---		
DOC-11.2	Does the SaMD rely on an owner/operator provided operating system?	No	---		
DOC-11.3	Is the SaMD hosted by the manufacturer?	No	---		
DOC-11.4	Is the SaMD hosted by the customer?	See Notes	Usually hosted in data centers of the customer		

Yes, No, N/A, or See Note

Note #

	MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION			IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
MPII-1	Can this device display, transmit, store, or modify personally identifiable information (e.g. electronic Protected Health Information (ePHI))?	Yes	---		AR-2	A.15.1.4
MPII-2	Does the device maintain personally identifiable information?	Yes	---		AR-2	A.15.1.4
MPII-2.1	Does the device maintain personally identifiable information temporarily in volatile memory (i.e., until cleared by power-off or reset)?	No	---		AR-2	A.15.1.4
MPII-2.2	Does the device store personally identifiable information persistently on internal media?	No	The data is stored on a mounted storage device like SAN/NAAS.			
MPII-2.3	Is personally identifiable information preserved in the device's non-volatile memory until explicitly erased?	See Notes	Log files may contain personally identifiable information. Rotation of log files automatically removes PHI.			
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?	See Notes	Log files may contain personally identifiable information. Rotation of log files automatically removes PHI.		AR-2	A.15.1.4
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	---		AR-2	A.15.1.4
MPII-2.7	Does the device maintain personally identifiable information when powered off, or during power service interruptions?	Yes	Product stores PHI on media (HDD) that does not need a permanent power service. The server hardware can be connected to an UPS. This helps to prevent the loss of data in transient memory during power service interruptions.		AR-2	A.15.1.4
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)?	No	---			
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	The data is stored on a mounted storage device like SAN/NAAS.		AR-2	A.15.1.4
MPII-3	Does the device have mechanisms used for the transmitting, importing/exporting of personally identifiable information?	Yes	---		AR-2	A.15.1.4
MPII-3.1	Does the device display personally identifiable information (e.g., video display, etc.)?	Yes	---		AR-2	A.15.1.4
MPII-3.2	Does the device generate hardcopy reports or images containing personally identifiable information?	Yes	---		AR-2	A.15.1.4
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.)?	No	---		AR-2	A.15.1.4
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.)?	No	---		AR-2	A.15.1.4
MPII-3.5	Does the device transmit/receive personally identifiable information via a wired network connection (e.g., RJ45, fiber optic, etc.)?	Yes	---		AR-2	A.15.1.4
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	Product does not provide integrated wireless connection. ePHI will only be transmitted via WiFi in case client machines are connected to eHealth Solutions by means of a wireless infrastructure available at the customer's site.		AR-2	A.15.1.4
MPII-3.7	Does the device transmit/receive personally identifiable information over an external network (e.g., Internet)?	See Notes	eHealth Solutions is not intended to be directly connected to public networks. eHealth Solutions' web portals can be made accessible e.g. via internet in customer-specific settings. For those cases, well-documented mandatory security measures such as a deployment behind a Reverse Proxy/Web Application Firewall and in different De-militarized Zones (DMZs) are provided to the customer.		AR-2	A.15.1.4
MPII-3.8	Does the device import personally identifiable information via scanning a document?	No	---			
MPII-3.9	Does the device transmit/receive personally identifiable information via a proprietary protocol?	No	---			
MPII-3.10	Does the device use any other mechanism to transmit, import or export personally identifiable information?	No	---		AR-2	A.15.1.4

	AUTOMATIC LOGOFF (ALOF)			IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
<i>The device's ability to prevent access and misuse by unauthorized users if device is left idle for a period of time.</i>						
ALOF-1	Can the device be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., auto-logout, session lock, password protected screen saver)?	Yes	---	Section 5.1, ALOF	AC-12	None
ALOF-2	Is the length of inactivity time before auto-logout/screen lock user or administrator configurable?	Yes	The web application UIs have a configurable session timeout. In addition, the logout capability of the portal can be used.	Section 5.1, ALOF	AC-11	A.11.2.8, A.11.2.9

AUDIT CONTROLS (AUDT)				IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
<i>The ability to reliably audit activity on the device.</i>						
AUDT-1	Can the medical device create additional audit logs or reports beyond standard operating system logs?	Yes	IHE-compliant ATNA Audit Logs are created.	Section 5.2, AUDT	AU-1	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
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?	No	—	Section 5.2, AUDT	AU-2	None
AUDT-2	Are events recorded in an audit log? If yes, indicate which of the following events are recorded in the audit log:	Yes	—	Section 5.2, AUDT	AU-2	None
AUDT-2.1	Successful login/logout attempts?	Yes	—	Section 5.2, AUDT	AU-2	None
AUDT-2.2	Unsuccessful login/logout attempts?	Yes	—	Section 5.2, AUDT	AU-2	None
AUDT-2.3	Modification of user privileges?	Yes	—	Section 5.2, AUDT	AU-2	None
AUDT-2.4	Creation/modification/deletion of users?	Yes	—	Section 5.2, AUDT	AU-2	None
AUDT-2.5	Presentation of clinical or PII data (e.g. display, print)?	Yes	—	Section 5.2, AUDT	AU-2	None
AUDT-2.6	Creation/modification/deletion of data?	Yes	—	Section 5.2, AUDT	AU-2	None
AUDT-2.7	Import/export of data from removable media (e.g. USB drive, external hard drive, DVD)?	Yes	—	Section 5.2, AUDT	AU-2	None
AUDT-2.8	Receipt/transmission of data or commands over a network or point-to-point connection?	Yes	—	Section 5.2, AUDT	AU-2	None
AUDT-2.8.1	Remote or on-site support?	See Notes	Not included in the product as no remote or on-site support feature is available in eHealth Solutions. The Remote Service Center provides audit logs for remote service activities.	Section 5.2, AUDT	AU-2	None
AUDT-2.8.2	Application Programming Interface (API) and similar activity?	Yes	—	Section 5.2, AUDT	AU-2	None
AUDT-2.9	Emergency access?	Yes	Emergency access is a feature that must be explicitly enabled in advance. Restrictions on document types that may be available in emergency access cases can be defined by the patient.	Section 5.2, AUDT	AU-2	None
AUDT-2.10	Other events (e.g., software updates)?	No	—	Section 5.2, AUDT	AU-2	None
AUDT-2.11	Is the audit capability documented in more detail?	Yes	—	Section 5.2, AUDT	AU-2	None
AUDT-3	Can the owner/operator define or select which events are recorded in the audit log?	No	Audit logs and events are predefined and cannot be changed. Well-established query interfaces exist for audit log analysis.	Section 5.2, AUDT	AU-2	None
AUDT-4	Is a list of data attributes that are captured in the audit log for an event available?	Yes	According to IHE ATNA	Section 5.2, AUDT	AU-2	None
AUDT-4.1	Does the audit log record date/time?	Yes	—	Section 5.2, AUDT	AU-2	None
AUDT-4.1.1	Can date and time be synchronized by Network Time Protocol (NTP) or equivalent time source?	Yes	Use of Secure NTP is recommended.	Section 5.2, AUDT	AU-2	None
AUDT-5	Can audit log content be exported?	Yes	—	Section 5.2, AUDT	AU-2	None
AUDT-5.1	Via physical media?	No	As downloadable export			
AUDT-5.2	Via IHE Audit Trail and Node Authentication (ATNA) profile to SEM?	Yes	—			
AUDT-5.3	Via other communications (e.g., external service device, mobile applications)?	Yes	—			
AUDT-5.4	Are audit logs encrypted in transit or on storage media?	Yes	—			
AUDT-6	Can audit logs be monitored/reviewed by owner/operator?	Yes	—			
AUDT-7	Are audit logs protected from modification?	Yes	—	Section 5.2, AUDT	AU-2	None
AUDT-7.1	Are audit logs protected from access?	Yes	—			
AUDT-8	Can audit logs be analyzed by the device?	Yes	—	Section 5.2, AUDT	AU-2	None

AUTHORIZATION (AUTH)				IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
<i>The ability of the device to determine the authorization of users.</i>						
AUTH-1	Does the device prevent access to unauthorized users through user login requirements or other mechanism?	Yes	—	Section 5.3, AUTH	IA-2	A.9.2.1
AUTH-1.1	Can the device be configured to use federated credentials management of users for authorization (e.g., LDAP, OAuth)?	Yes	—	Section 5.3, AUTH	IA-2	A.9.2.1
AUTH-1.2	Can the customer push group policies to the device (e.g., Active Directory)?	Yes	—	Section 5.3, AUTH	IA-2	A.9.2.1
AUTH-1.3	Are any special groups, organizational units, or group policies required?	No	—	Section 5.3, AUTH	IA-2	A.9.2.1
AUTH-2	Can users be assigned different privilege levels based on 'role' (e.g., user, administrator, and/or service, etc.)?	Yes	—	Section 5.3, AUTH	IA-2	A.9.2.1
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	Access to PHI is granted by the access control system based on user authentication where local root access does not lead to application-specific administrative privileges.	Section 5.3, AUTH	IA-2	A.9.2.1
AUTH-4	Does the device authorize or control all API access requests?	Yes	—	Section 5.3, AUTH	IA-2	A.9.2.1
AUTH-5	Does the device run in a restricted access mode, or 'kiosk mode', by default?	See Notes	Permissions are granted on a user and role level.			

CYBER SECURITY PRODUCT UPGRADES (CSUP)				IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
<i>The ability of on-site service staff, remote service staff, or authorized customer staff to install/upgrade device's security patches.</i>						
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	—			
CSUP-2	Does the device contain an Operating System? If yes, complete 3.1.2.4.	Yes	—			
CSUP-2.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	Yes	—			
CSUP-2.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	No	—			
CSUP-2.3	Does the device have the capability to receive remote installation of patches or software updates?	Yes	Siemens Remote Service infrastructure provides secure means of downloading security patches and application-specific updates. Additionally, application-specific security patches can be provided by a software repository to be propagated manually. In case Siemens Remote Service infrastructure cannot be utilized, a service engineer or customer IT administrator has to install the required security patches and updates. Operating system patches can be installed from official sources.			
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?	Yes	—			
CSUP-3	Does the device contain Drivers and Firmware? If yes, complete 3.1.3.4.	No	—			
CSUP-3.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	N/A	—			
CSUP-3.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	N/A	—			



CSUP-3.3	Does the device have the capability to receive remote installation of patches or software updates?	N/A	—			
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?	N/A	—			
CSUP-4	Does the device contain Anti-Malware Software? If yes, complete 4.1.4.4.	See Notes	Anti-malware software is recommended to be installed by customer but not included in product. A scripting interface is available to allow anti-malware scans on a per-document basis during registration and download. Malware scanners are to be provided by the customer.			
CSUP-4.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	N/A	—			
CSUP-4.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	N/A	—			
CSUP-4.3	Does the device have the capability to receive remote installation of patches or software updates?	N/A	—			
CSUP-4.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	N/A	—			
CSUP-5	Does the device contain Non-Operating System commercial off-the-shelf components? If yes, complete 5.1-5.4.	See Notes	Third-party components such as libraries and application servers are included in the software release and provided as operating system packages.			
CSUP-5.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	N/A	—			
CSUP-5.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	N/A	—			
CSUP-5.3	Does the device have the capability to receive remote installation of patches or software updates?	N/A	—			
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?	N/A	—			
CSUP-6	Does the device contain other software components (e.g., asset management software, license management)? If yes, please provide details or reference in notes and complete 6.1-6.4.	No	—			
CSUP-6.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	N/A	—			
CSUP-6.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	N/A	—			
CSUP-6.3	Does the device have the capability to receive remote installation of patches or software updates?	N/A	—			
CSUP-6.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	N/A	—			
CSUP-7	Does the manufacturer notify the customer when updates are approved for installation?	See Notes	Customer is notified via Remote Service Center.			
CSUP-8	Does the device perform automatic installation of software updates?	See Notes	Updates of eHealth Solutions applications are not automatically installed. Automatic operating system updates are configured per default.			
CSUP-9	Does the manufacturer have an approved list of third-party software that can be installed on the device?	See Notes	There are no restrictions on third-party components that can be installed on the machines.			
CSUP-10	Can the owner/operator install manufacturer-approved third-party software on the device themselves?	See Notes	Installation of third-party software is not restricted by the manufacturer.			
CSUP-10.1	Does the system have mechanism in place to prevent installation of unapproved software?	See Notes	Operating system (OS) verification of software packages is enabled per default. Application updates are provided as OS packages by RPM Package Manager (RPM).			
CSUP-11	Does the manufacturer have a process in place to assess device vulnerabilities and updates?	Yes	Vulnerabilities of third-party components are continuously monitored. Internal penetration tests are carried out regularly.			
CSUP-11.1	Does the manufacturer provide customers with review and approval status of updates?	Yes	Software upgrades are provided only after internal verification and clearance which is transparently communicated to customers.			
CSUP-11.2	Is there an update review cycle for the device?	Yes	Release Upgrades are provided regularly. Bug fixes for software defects on demand. Both after internal verification and clearance.			

HEALTH DATA DE-IDENTIFICATION (DIDT)			IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
<i>The ability of the device to directly remove information that allows identification of a person.</i>					
DIDT-1	Does the device provide an integral capability to de-identify personally identifiable information?	Yes	System relies on distributed services where PHI is linked to patient data via a unique and irreversible identifier. Services use this identifier to link PHI to demographic data. Thus, pseudonymization is supported implicitly.	None	ISO 27038
DIDT-1.1	Does the device support de-identification profiles that comply with the DICOM standard for de-identification?	N/A		None	ISO 27038

DATA BACKUP AND DISASTER RECOVERY (DTBK)			IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
<i>The ability to recover after damage or destruction of device data, hardware, software, or site configuration information.</i>					
DTBK-1	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)?	Yes	—		
DTBK-2	Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer?	No	—	Section 5.7, DTBK	CP-9 A.12.3.1
DTBK-3	Does the device have an integral data backup capability to removable media?	Yes	The system should be integrated in existing backup and recovery infrastructures. A detailed backup and recovery concept is elaborated with the customer for site-specific operations.	Section 5.7, DTBK	CP-9 A.12.3.1
DTBK-4	Does the device have an integral data backup capability to remote storage?	Yes			
DTBK-5	Does the device have a backup capability for system configuration information, patch restoration, and software restoration?	Yes	Entire machine backup via virtualization environment is handled by the customer. Administration Manuals provide detailed references.		
DTBK-6	Does the device provide the capability to check the integrity and authenticity of a backup?	See Notes	Integrity and authenticity for database backups is provided by DBMS tools.	Section 5.7, DTBK	CP-9 A.12.3.1

EMERGENCY ACCESS (EMRG)			IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
<i>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.</i>					

EMRG-1	Does the device incorporate an emergency access (i.e. "break-glass") feature?	Yes	Emergency access is a feature that must be explicitly enabled in advance. System provides special PurposeOfUse element in SAML Token to indicate emergency access. Emergency access requires successful authentication and is subject to audit logging. Restrictions on document types that may be available in emergency access cases can be defined by the patient.	Section 5.8, EMRG	SI-17	None
--------	---	-----	---	-------------------	-------	------

HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU)				IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
<i>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.</i>						
IGAU-1	Does the device provide data integrity checking mechanisms of stored health data (e.g., hash or digital signature)?	Yes		Section 5.9, IGAU	SC-28	A.18.1.3
IGAU-2	Does the device provide error/failure protection and recovery mechanisms for stored health data (e.g., RAID-5)?	Yes	—	Section 5.9, IGAU	SC-28	A.18.1.3

MALWARE DETECTION/PROTECTION (MLDP)				IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
<i>The ability of the device to effectively prevent, detect and remove malicious software (malware).</i>						
MLDP-1	Is the device capable of hosting executable software?	Yes	—	Section 5.10, MLDP		
MLDP-2	Does the device support the use of anti-malware software (or other anti-malware mechanisms)? Provide details or reference in notes.	Yes	—	Section 5.10, MLDP	SI-3	A.12.2.1
MLDP-2.1	Does the device include anti-malware software by default?	No	—	Section 5.10, MLDP	CM-5	A.9.2.3, A.9.4.5, A.12.1.2, A.12.1.4, A.12.5.1
MLDP-2.2	Does the device have anti-malware software available as an option?	See Notes	Anti-malware software is recommended to be installed by customer but not included in product. A scripting interface is available to allow anti-malware scans on a per-document basis during registration and download. Malware scanners are to be provided by the customer.	Section 5.10, MLDP	AU-6	A.12.4.1, A.16.1.2, A.16.1.4
MLDP-2.3	Does the device documentation allow the owner/operator to install or update anti-malware software?	Yes	—	Section 5.10, MLDP	CP-10	A.17.1.2
MLDP-2.4	Can the device owner/operator independently (re-)configure anti-malware settings?	Yes	—	Section 5.10, MLDP	AU-2	None
MLDP-2.5	Does notification of malware detection occur in the device user interface?	See Notes	A failed download is indicated in the user interface if a malware scanner detects malware in a downloaded document. For this purpose, malware scanners must be enabled and configured by customer. See above.			
MLDP-2.6	Can only manufacturer-authorized persons repair systems when malware has been detected?	Yes	—			
MLDP-2.7	Are malware notifications written to a log?	N/A	—			
MLDP-2.8	Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)?	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	—	Section 5.10, MLDP	SI-2	A.12.6.1, A.14.2.2, A.14.2.3, A.16.1.3
MLDP-4	Does the device employ application whitelisting that restricts the software and services that are permitted to be run on the device?	No	—	Section 5.10, MLDP	SI-3	A.12.2.1
MLDP-5	Does the device employ a host-based intrusion detection/prevention system?	See Notes	Host-base IDS/IPS can be configured by customer.	Section 5.10, MLDP	SI-4	None
MLDP-5.1	Can the host-based intrusion detection/prevention system be configured by the customer?	N/A	—	Section 5.10, MLDP	CM-7	A.12.5.1
MLDP-5.2	Can a host-based intrusion detection/prevention system be installed by the customer?	Yes	—	Section 5.10, MLDP		

NODE AUTHENTICATION (NAUT)				IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
<i>The ability of the device to authenticate communication partners/nodes.</i>						
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	—	Section 5.11, NAUT	SC-23	None
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	Detailed recommendations are provided on how the product is to be operated in protected network segments of the customer.	Section 5.11, NAUT	SC-7	A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.3
NAUT-2.1	Is the firewall ruleset documented and available for review?	N/A	—			
NAUT-3	Does the device use certificate-based network connection authentication?	Yes	According to IHE ATNA with the latest and highest-rated algorithms and protocols.			

CONNECTIVITY CAPABILITIES (CONN)				IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
<i>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.</i>						
CONN-1	Does the device have hardware connectivity capabilities?	See Notes	Product is hosted as virtual machine. Physical networking and storage connections depend on the underlying host machine. The product's operating system configures virtualized Ethernet connections.			
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?	See Notes	Product is hosted as virtual machine. Physical networking connections depend on the underlying host machine. The product's operating system configures virtualized Ethernet connections.			
CONN-1.2.1	Does the device have available RJ45 Ethernet ports?	Yes	Virtualized Ethernet			
CONN-1.2.2	Does the device have available USB ports?	See Notes	USB Ports are not used for the product; however, they might exist on the host machine running the virtual machines.			
CONN-1.2.3	Does the device require, use, or support removable memory devices?	No	—			
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	List is provided in the Product and Solution Security Whitepaper.			
CONN-3	Can the device communicate with other systems within the customer environment?	Yes	Via DICOM, HL7, Web Services. See details in Product and Solution Security Whitepaper.			
CONN-4	Can the device communicate with other systems external to the customer environment (e.g., a service host)?	No	—			
CONN-5	Does the device make or receive API calls?	Yes	A Web Service API (so-called Connectivity Package) is available via HTTPS (TLS-encrypted). HL7 FHIR interfaces are also available via HTTPS.			

CONN-6	Does the device require an internet connection for its intended use?	No	—			
CONN-7	Does the device support Transport Layer Security (TLS)?	Yes	—			
CONN-7.1	Is TLS configurable?	Yes	—			
CONN-8	Does the device provide operator control functionality from a separate device (e.g., telemedicine)?	No	—			

PERSON AUTHENTICATION (PAUT)				IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
<i>The ability to configure the device to authenticate users.</i>						
PAUT-1	Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)?	Yes	—	Section 5.12, PAUT	IA-2	A.9.2.1
PAUT-1.1	Does the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)?	Yes	—	Section 5.12, PAUT	IA-2	A.9.2.1
PAUT-2	Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, etc.)?	Yes	Built-in or external SAML 2.0-compliant identity provider (IDPs) can be used for user authentication.	Section 5.12, PAUT	IA-5	A.9.2.1
PAUT-3	Is the device configurable to lock out a user after a certain number of unsuccessful login attempts?	Yes	—	Section 5.12, PAUT	IA-2	A.9.2.1
PAUT-4	Are all default accounts (e.g., technician service accounts, administrator accounts) listed in the documentation?	Yes	—	Section 5.12, PAUT	SA-4(5)	A.14.1.1, A.14.2.7, A.14.2.9, A.15.1.2
PAUT-5	Can all passwords be changed?	Yes	—	Section 5.12, PAUT		
PAUT-6	Is the device configurable to enforce creation of user account passwords that meet established (organization specific) complexity rules?	Yes	—	Section 5.12, PAUT	IA-2	A.9.2.1
PAUT-7	Does the device support account passwords that expire periodically?	Yes	—			
PAUT-8	Does the device support multi-factor authentication?	Yes	Via TOTP			
PAUT-9	Does the device support single sign-on (SSO)?	Yes	Via SAML and digitally signed URL	Section 5.12, PAUT	IA-2	A.9.2.1
PAUT-10	Can user accounts be disabled/locked on the device?	Yes	—	Section 5.12, PAUT	IA-2	A.9.2.1
PAUT-11	Does the device support biometric controls?	No	—	Section 5.12, PAUT	IA-2	A.9.2.1
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?	See Notes	Credentials can be persisted in database or taken from an existing LDAP directory service.			
PAUT-14.1	Are credentials stored using a secure method?	Yes	Credentials are stored as cryptographic hashes including so called "salt" parameters as an efficient countermeasure against brute-force attacks.			

PHYSICAL LOCKS (PLOK)				IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
<i>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</i>						
PLOK-1	Is the device software only? If yes, answer "N/A" to remaining questions in this section.	Yes	—	Section 5.13, PLOK	PE-3(4)	A.11.1.1, A.11.1.2, A.11.1.3
PLOK-2	Are all device components maintaining personally identifiable information (other than removable media) physically secure (i.e., cannot remove without tools)?	N/A	Hardware server rack should be locked against unauthorized removal by the customer.	Section 5.13, PLOK	PE-3(4)	A.11.1.1, A.11.1.2, A.11.1.3
PLOK-3	Are all device components maintaining personally identifiable information (other than removable media) physically secured behind an individually keyed locking device?	N/A	—	Section 5.13, PLOK	PE-3(4)	A.11.1.1, A.11.1.2, A.11.1.3
PLOK-4	Does the device have an option for the customer to attach a physical lock to restrict access to removable media?	N/A	Product is operated in virtualized environments.	Section 5.13, PLOK	PE-3(4)	A.11.1.1, A.11.1.2, A.11.1.3

ROADMAP FOR THIRD-PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP)				IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
<i>Manufacturer's plans for security support of third-party components within the device's life cycle.</i>						
RDMP-1	Was a secure software development process, such as ISO/IEC 27034 or IEC 62304, followed during product development?	Yes	—	Section 5.14, RDMP	CM-2	None
RDMP-2	Does the manufacturer evaluate third-party applications and software components included in the device for secure development practices?	Yes	Siemens vulnerability monitoring systems are used for periodic check of third-party components. A complete list of third-party software and libraries is included in the Release Notes of the product.	Section 5.14, RDMP	CM-8	A.8.1.1, A.8.1.2
RDMP-3	Does the manufacturer maintain a web page or other source of information on software support dates and updates?	Yes	—	Section 5.14, RDMP	CM-8	A.8.1.1, A.8.1.2
RDMP-4	Does the manufacturer have a plan for managing third-party component end-of-life?	Yes	—	Section 5.14, RDMP	CM-8	A.8.1.1, A.8.1.2

SOFTWARE BILL OF MATERIALS (SBOM)				IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
<i>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.</i>						
SBOM-1	Is the SBOM for this product available?	Yes	—			
SBOM-2	Does the SBOM follow a standard or common method in describing software components?	Yes	—			
SBOM-2.1	Are the software components identified?	Yes	—			
SBOM-2.2	Are the developers/manufacturers of the software components identified?	Yes	—			
SBOM-2.3	Are the major version numbers of the software components identified?	Yes	—			
SBOM-2.4	Are any additional descriptive elements identified?	Yes	—			
SBOM-3	Does the device include a command or process method available to generate a list of software components installed on the device?	See Notes	SBOM is part of the release documentation that is shipped along with the product.			
SBOM-4	Is there an update process for the SBOM?	Yes	—			

SYSTEM AND APPLICATION HARDENING (SAHD)				IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
<i>The device's inherent resistance to cyber attacks and malware.</i>						
SAHD-1	Is the device hardened in accordance with any industry standards?	See Notes	Hardening of operating system is recommended to be carried out by customer according to specific internal guidelines.	Section 5.15, SAHD	AC-17(2)/IA-3	A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2/None
SAHD-2	Has the device received any cybersecurity certifications?	Yes	Penetration tests have been carried out by Siemens.	Section 5.15, SAHD	SA-12(10)	A.14.2.7, A.15.1.1, A.15.1.2, A.15.1.3
SAHD-3	Does the device employ any mechanisms for software integrity checking?	Yes	Software is installed as RPM packages which have integrity checks enabled per default.			
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	Software is installed as RPM packages which have integrity checks enabled per default.			

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	The device is application software only and does not include any changes at installation to other OS programs and HW.	Section 5.15, SAHD	CM-8	A.8.1.1, A.8.1.2
SAHD-4	Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)?	Yes	The owner/operator can apply RPM-based integrity checks.	Section 5.15, SAHD	AC-3	A.6.2.2, A.9.1.2, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.1, A.14.1.2, A.14.1.3, A.18.1.3
SAHD-5	Is the system configurable to allow the implementation of file-level, patient level, or other types of access controls?	Yes	—	Section 5.15, SAHD	CM-7	A.12.5.1*
SAHD-5.1	Does the device provide role-based access controls?	Yes	—	Section 5.15, SAHD	CM-7	A.12.5.1*
SAHD-6	Are any system or user accounts restricted or disabled by the manufacturer at system delivery?	Yes	—	Section 5.15, SAHD	CM-8	A.8.1.1, A.8.1.2
SAHD-6.1	Are any system or user accounts configurable by the end user after initial configuration?	Yes	—	Section 5.15, SAHD	CM-7	A.12.5.1*
SAHD-6.2	Does this include restricting certain system or user accounts, such as service technicians, to least privileged access?	Yes	—	Section 5.15, SAHD	CM-7	A.12.5.1*
SAHD-7	Are all shared resources (e.g., file shares) which are not required for the intended use of the device disabled?	Yes	—	Section 5.15, SAHD	CM-7	A.12.5.1*
SAHD-8	Are all communication ports and protocols that are not required for the intended use of the device disabled?	Yes	—	Section 5.15, SAHD	SA-18	None
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	—	Section 5.15, SAHD	CM-6	None
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	—	Section 5.15, SAHD	SI-2	A.12.6.1, A.14.2.2, A.14.2.3, A.16.1.3
SAHD-11	Can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?	See Notes	The configuration of boot devices is handled by the underlying virtualization environment. The virtual machine does not boot from devices other than the pre-configured ones.			
SAHD-12	Can unauthorized software or hardware be installed on the device without the use of physical tools?	Yes	The manufacturer does not restrict additional software that may be installed by the customer.			
SAHD-13	Does the product documentation include information on operational network security scanning by users?	See Notes	Network scanning does not affect the product.			
SAHD-14	Can the device be hardened beyond the default provided state?	Yes	Additional hardening is recommended.			
SAHD-14.1	Are instructions available from vendor for increased hardening?	No	—			
SAHD-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	—			

SECURITY GUIDANCE (SGUD)			IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
<i>Availability of security guidance for operator and administrator of the device and manufacturer sales and service.</i>					
SGUD-1	Does the device include security documentation for the owner/operator?	Yes	—	AT-2/PL-2	A.7.2.2, A.12.2.1/A.14.1.1
SGUD-2	Does the device have the capability, and provide instructions, for the permanent deletion of data from the device or media?	Yes	—	MP-6	A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7
SGUD-3	Are all access accounts documented?	Yes	Default accounts are well documented. Additional accounts can be created by operators.	AC-6JA-2	A.9.1.2, A.9.2.3, A.9.4.4, A.9.4.5/A.9.2.1
SGUD-3.1	Can the owner/operator manage password control for all accounts?	Yes	—		
SGUD-4	Does the product include documentation on recommended compensating controls for the device?	Yes	Guidelines for secure configuration according to the intended operational environment are available.		

HEALTH DATA STORAGE CONFIDENTIALITY (STCF)			IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013	
<i>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.</i>						
STCF-1	Can the device encrypt data at rest?	See Notes	Data at rest can be encrypted using - document-based encryption - database encryption - storage encryption. Encryption must be configured by the customer.	Section 5.17, STCF	SC-28	A.8.2.3
STCF-1.1	Is all data encrypted or otherwise protected?	See Notes	See above			
STCF-1.2	Is the data encryption capability configured by default?	No	—			
STCF-1.3	Are instructions available to the customer to configure encryption?	Yes	—			
STCF-2	Can the encryption keys be changed or configured?	Yes	—	Section 5.17, STCF	SC-28	A.8.2.3
STCF-3	Is the data stored in a database located on the device?	No	—			
STCF-4	Is the data stored in a database external to the device?	Yes	—			

TRANSMISSION CONFIDENTIALITY (TXCF)			IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013	
<i>The ability of the device to ensure the confidentiality of transmitted personally identifiable information.</i>						
TXCF-1	Can personally identifiable information be transmitted only via a point-to-point dedicated cable?	No	—	Section 5.18, TXCF	CM-7	A.12.5.1
TXCF-2	Is personally identifiable information encrypted prior to transmission via a network or removable media?	Yes	Network communication is secured using SSL/TLS.	Section 5.18, TXCF	CM-7	A.12.5.1
TXCF-2.1	If data is not encrypted by default, can the customer configure encryption options?	Yes	—			
TXCF-3	Is personally identifiable information transmission restricted to a fixed list of network destinations?	Yes	—	Section 5.18, TXCF	CM-7	A.12.5.1
TXCF-4	Are connections limited to authenticated systems?	Yes	According to IHE ATNA	Section 5.18, TXCF	CM-7	A.12.5.1
TXCF-5	Are secure transmission methods supported/implemented (DICOM, HL7, IEEE 11073)?	Yes	—			

TRANSMISSION INTEGRITY (TXIG)			IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013	
<i>The ability of the device to ensure the integrity of transmitted data.</i>						
TXIG-1	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission?	Yes	Document metadata provide checksums on document basis. System solely uses TLS 1.2-encrypted communication paths, which implies authenticity of transmitted data.	Section 5.19, TXIG	SC-8	A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3
TXIG-2	Does the device include multiple sub-components connected by external cables?	No	—			

REMOTE SERVICE (RMOT)			IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013	
<i>Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.</i>						
RMOT-1	Does the device permit remote service connections for device analysis or repair?	See Notes	Remote Service is handled primarily via Siemens Remote Service Center. Thereby, a secure connection is initiated.		AC-17	A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2

# 8 Abbreviations

**Table 5:** List of Technical Abbreviations

ADT	Admit, Discharge & Transfer (HL7)
ATNA	Audit Trail and Node Authentication
APPC	Advanced Patient Privacy Consents
CDA	Clinical Document Architecture
DICOM	Digital Imaging and Communications in Medicine
ePHI	Electronic Protected Health Information
FHIR	Fast Healthcare Interoperability Resources
HIPAA	Health Insurance Portability and Accountability Act
HL7	Health Level 7
HTTPS	Hypertext Transfer Protocol Secure
IHE	Integrating the Healthcare Enterprise
IUA	Internet User Authorization
JWT	JSON Web Token
LDAP	Lightweight Directory Access Protocol
MDM	Medical Document Management
MDS <sup>2</sup>	Manufacturer Disclosure Statement
NTP	Network Time Protocol
PHI	Protected Health Information
PII	Personally Identifiable Information
SAML	Security Assertion Markup Language
SNTP	Simple Network Time Protocol
SOAP	Simple Object Access Protocol
SSH	Secure Shell
SSO	Single Sign-on
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
WAF	Web Application Firewall
WSS	WebSocket Secure
XACML	Extensible Access Control Markup Language
XDS	Direct Save Protocol
XML	Extensible Markup Language
XSS	Cross-Site Scripting
XUA	Cross-Enterprise User Assertion

## 8.1 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 (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.

## 8.2 Statement on FDA Cybersecurity Guidance

Siemens Healthineers will follow cybersecurity guidance issued by the FDA as appropriate. Siemens Healthineers recognizes the principle described in FDA cybersecurity guidance that an effective cybersecurity framework is a shared responsibility among multiple stakeholders (e.g., medical device manufacturers, health care facilities, patients and providers), and is committed to drawing on its innovation, engineering and pioneering skills in collective efforts designed to prevent, detect and respond to new and emerging cybersecurity threats. While FDA cybersecurity guidance is informative as to adopting a risk-based approach to addressing potential patient harm, it is not binding, and alternative approaches may be used to satisfy FDA regulatory requirements.

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

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

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

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

Siemens reserves the right to modify the design, packaging, specifications and options described herein without prior notice. Please contact your local Siemens sales representative for the most current information. In the interest of complying with legal requirements concerning the environmental compatibility of our products (protection of natural resources and waste conservation), we recycle certain components. Using the same extensive quality assurance measures as for factory-new components, we guarantee the quality of these recycled components.

---

**Distributed by**

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

**Legal Manufacturer**

ITH icoserve technology for healthcare GmbH  
Innrain 98  
6020 Innsbruck  
Austria  
Phone: +43 512 89059

*Made in Austria*