eHealth Solutions / Release VA37A / 2019-10-30 / Revision 93838

eHealth Solutions Product and Solution Security White Paper

SIEMENS Healthineers

Contents

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 medical devices. 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.

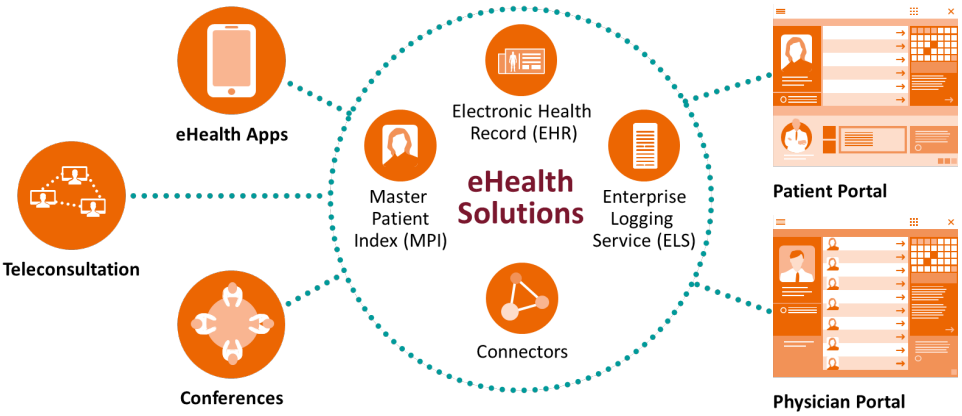
1.4 Contacting Siemens Healthineers about Product and Solution Security

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

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

2 Basic Information

Figure 1: Overview of eHealth Solutions services and applications



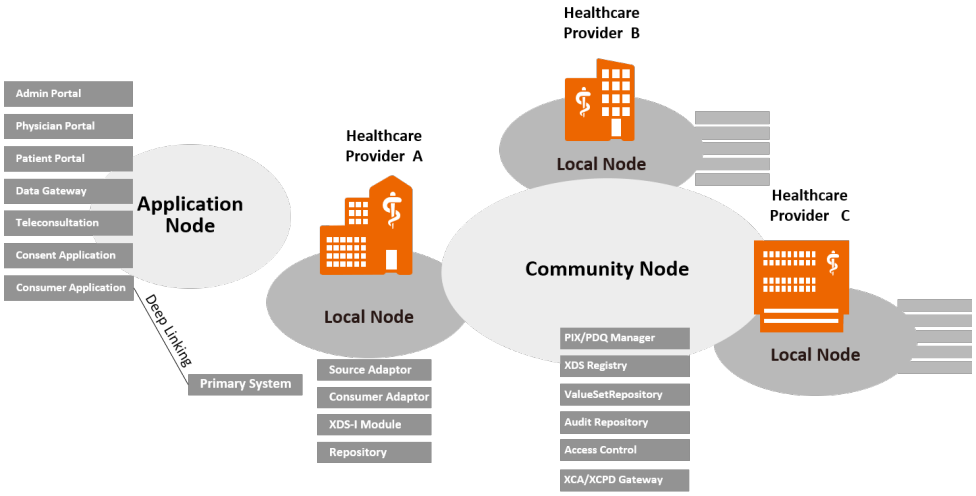
eHealth Solutions connects institutions for cooperative care and optimized communication.

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 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
CPU	4 Core
RAM	32 GB
Hard Disk	50 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.

2.3 Operating Systems

2.3.1 Client

There are no special operating system requirements for clients.

2.3.2 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 ≥ 60
- Mozilla Firefox ≥ 52
- Microsoft Edge ≥ 40
- Microsoft Internet Explorer ≥ 11

2.3.3 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.

2.3.4 Server

- Operating System: Red Hat Enterprise Linux 7 (7.4-7.x)
- Database Management System: Oracle Database 11gR2, 12c, 12cR2

2.3.5 Hypervisors

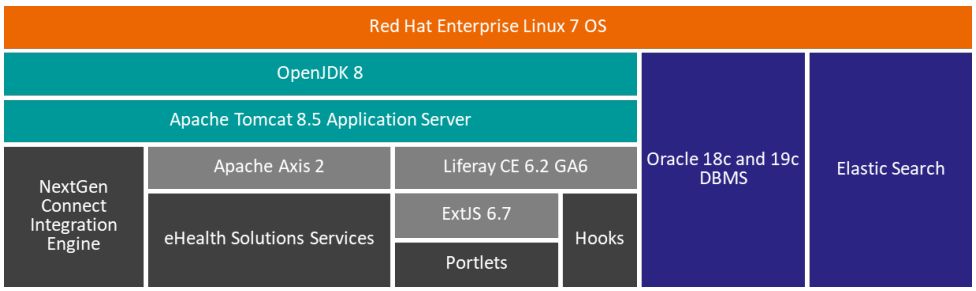
eHealth Solutions can be deployed in a virtualization environment. The following hypervisors are supported:

- VMware vSphere ≥ 5.0
- Hyper-V 2012 R2

2.4 Third-party Software

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

Figure 3: Third-party software in eHealth Solutions.



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

2.5 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).

2.6 User Account Information

The following types of users exist:

- Patients
- Healthcare professionals
- Administrative staff for clearing operations, etc.

2.7 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.

2.8 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.

2.9 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 then 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.
Form Processor	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.

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 4: Network Connections Including Internal Communication and Connectivity with Primary Systems

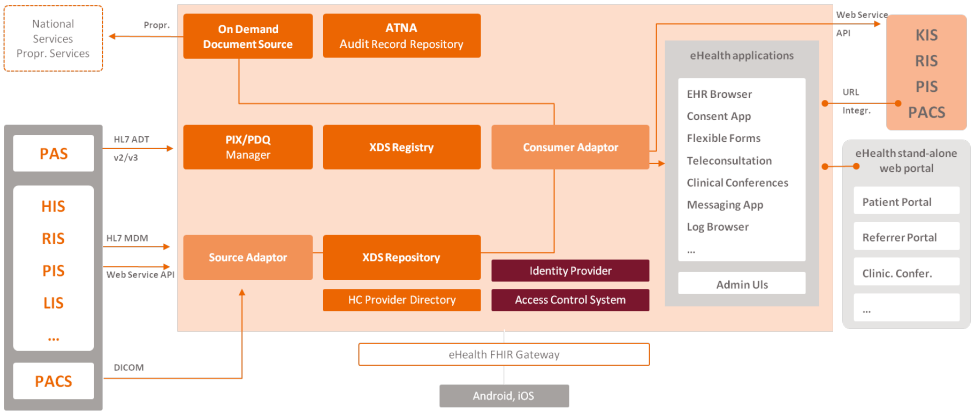


Table 3

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 physicans, patients, admins	Inbound	HTTPS
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

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 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.

4.3 Authentication and Authorization Controls

4.3.1 Authentication

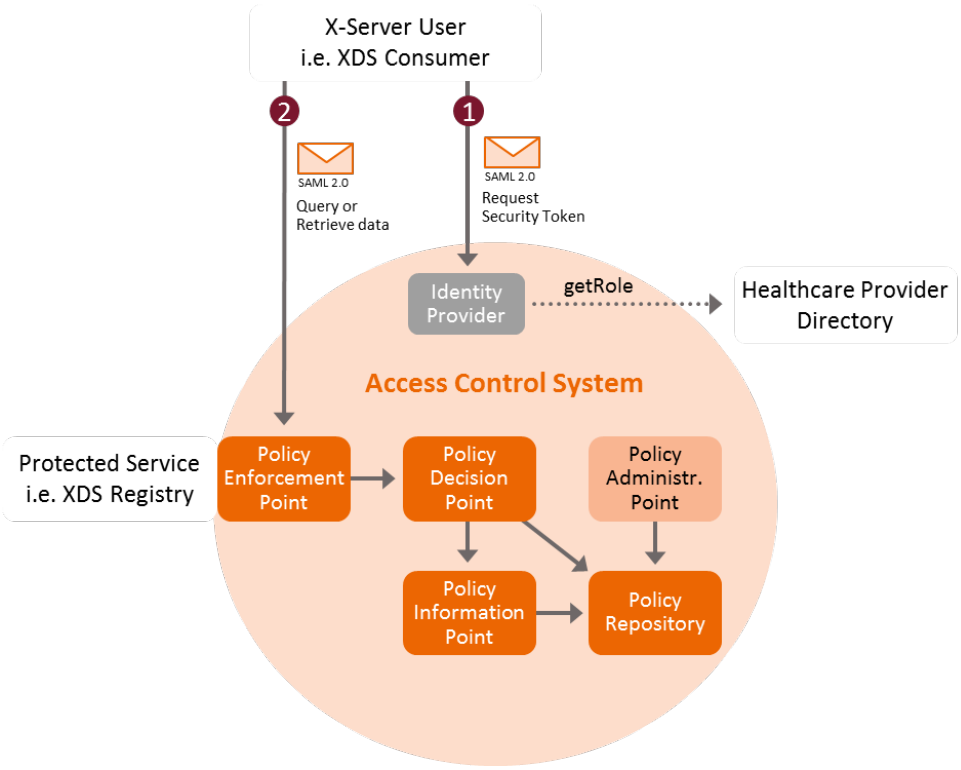
- User authentication and role information are handled by a SAML 2.0- and IHE XUA-compliant Identity Provider (IdP).
- User and role information is submitted from a trusted primary system (e.g. HIS, CIS) authenticated by client certificates.
- Manual user management via portal applications.
- Automatic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

Figure 5: Authentication via Built-in or External Identity Provider

4.3.2 Authorization

- User authorization is based on XACML policies that offer a state-of-the-art role- and context-based access control system.
- 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.

Figure 6: eHealth Solutions Access Control System Including Authentication via SAML Identity Provider



4.4 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.

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 4.4), 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`) 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**	› Covered by the security mechanism of the portal application. › Additionally: Input validation and usage of parametrized stored queries for the object-relational data mapper. › External Security Audits have placed special emphasis on robustness against injection attacks.
A2:2017	**Broken Authentication and Session Management**	Covered by the security mechanism of the portal application by usage of configurable, well-established authentication mechanisms such as: › LDAP › Active Directory › OpenSSO › OpenID › SAML 2.0 › Generation and persistence of user credentials via strong cryptography › Multi-factor authentication and Single-Sign-On compliant with IHE XUA

Table 4:

Table 4:

Criterion		Description
A3:2017	**Sensitive Data Exposure**	› 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. › Transport encryption compliant with IHE ATNA requiring secure algorithms and high key length.
A4:2017	**XML External Entity (XXE)**	XXE protection is provided by: › Server-side stylesheet rendering and input validation. › Continuous checks of XML documents such as CDA documents or stylesheets against schemata.
A5:2017	**Broken Access Control**	› XACML-compliant Access Control System with flexible configuration of policies to reflect patient consent declarations. › Compliant with IHE Access Control Requirements. › Covered by the security mechanism of the portal application as well as by role- and context-based authorization.
A6:2017	**Security Mis-configuration**	› Covered by the security mechanism of the portal application by usage of well-established architectural design (security by design) for separation of components. › Usage of most recent versions and security patches. › Checklists for productive installations which comprise: › Installation of no other than required packages › Deactivation of unused ports › Solely encrypted communication › Observance of customer-specific requirements concerning authentication policies (password length and complexity, Single Sign-On, multifactor authentication).
A7:2017	**Cross–Site Scripting** (XSS)	› Covered by the security mechanism of the portal application by input validation and additionally consequent escaping of output content. › External Security Audits have placed special emphasis on robustness against XSS attacks.
A8:2017	**Insecure Deserialization**	Usage of well-established XML bindings as well as strict type checks against XMS schemata.
A9:2017	**Using Components with Known Vulnerabilities**	› Continuous monitoring and reaction to known vulnerabilities. › Continuous monitoring of vulnerability lists. › Web-based management interfaces allow easy-to-use update with minimal downtime.

Table 4:

Table 4:

Criterion		Description
A10:2017	**Insufficient Logging & Monitoring**	› Audit Logging complaint to IHE ATNA Secure Node Requirements. › Detailed, distributed technical logs. › Web-based reports from the ATNA Audit Record Repository. › Optional integration of fraud-detection mechanisms. › Secure time synchronization compliant with IHE CT Secure Time Client/ Server.

4.5 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.

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.

4.6 Network Controls

- The system is designed to make limited use of network ports and protocols.
- A detailed firewalling concept is discussed with the customer for site-specific operations.

4.7 Physical Protection

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.

4.8 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.

4.9 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.

4.10 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

4.11 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.

4.12 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.
- Security aspects of installation are described in the Administrator Manual.

4.13 Incident Response Management

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

4.14 HIPAA Conformance Statement

Manufacturer Disclosure Statement for Medical Device Security – MDS[2]				
DEVICE DESCRIPTION				
Device Category	Manufacture ITH-icoserve Ges.m.b.H	Document ID eHealth Solutions VA37A HIPAA Compliance Statement (MDS2 Form)	Document Release Date 2019-10-30	
Device Model eHealth Solutions	Software Revision VA37A		Software Release Date 2019-10-30	
Manufacturer or Representative Contact Information	Company Name ITH-icoserve technology for healthcare Ges.m.b.H Representative Name/Position Dr. Bernhard Hirsch / Managing director	Manufacturer Contact Information Innrain 98 6020 Innsbruck Austria		
Intended use of **device** in network-connected environment:				
The intention of the device is to provide services, applications and tools for secure, cross-enterprise exchange of patient-related medical data (HIE solution).				
MANAGEMENT OF PRIVATE DATA				
Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.			Yes, No, N/A, or See Note	Note #
A	Can this **device** display, transmit, or maintain **private data** (including **electronic Protected Health Information** [ePHI])?		Yes	—
B	Types of **private data** elements that can be maintained by the **device**:			
B.1	Demographic (e.g., name, address, location, unique identification number)?		Yes	1
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**?	No	—
B.6	Personal financial information?	No	—
C	Maintaining **private data** — Can the **device**:		
C.1	Maintain **private data** temporarily in volatile memory (i.e., until cleared by power-off or reset)?	Yes	—
C.2	Store **private data** persistently on local media?	Yes	—
C.3	Import/export **private data** with other systems?	Yes	—
C.4	Maintain **private data** during power service interruptions?	Yes	2
D	Mechanisms used for the transmission, import/export 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**?	No	—
D.3	Retrieve **private data** from or record **private data** to **removable media** (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick, etc.)?	No	—
D.4	Transmit/receive or import/export **private data** via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire, etc.)?	No	—
D.5	Transmit/receive **private data** via 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., WiFi, Bluetooth, infrared, etc.)?	No	3
D.7	Import **private data** via scanning?	No	—
D.8	Other?	No	—
Management of Private Data notes:	1. PHI maintained by the system depends on the content of the clinical document and on the information provided by a connected Source Information System (typically a Clinical Information System). 2. Product stores PHI on media (HDD) that does not need a permanent power service. The server hardware can be connected to a UPS. This helps to prevent the loss of data in transient memory during power service interruptions. 3. Product does not provide integrated wireless connection. ePHI is only transmitted via WiFi in case client machines are connected to eHealth Solutions by means of a wireless infrastructure available at the customer's site.		

SECURITY CAPABILITIES

Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #

1	AUTOMATIC LOGOFF (ALOF) The **device**'s ability to prevent access and misuse by unauthorized **users** if **device** is left idle for a period of time.		
1-1	Can the **device** be configured to force reauthorization of logged-in **user**(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password-protected screen saver)?	Yes	—
1-1.1	Is the length of inactivity time before auto-logoff/screen lock **user** or administrator configurable? (Indicate time [fixed or configurable range] in notes.)	Yes	1
1-1.2	Can auto-logoff/screen lock be manually invoked (e.g., via a shortcut key or proximity sensor, etc.) by the **user**?	Yes	1
ALOF notes:	1. The web application UIs have a configurable session timeout. In addition, the logout capability of the portal can be used.		
2	AUDIT CONTROLS (AUDT) 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 recording 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	—
2-2.5.1	**Remote service** activity	Yes	1
2-2.6	Other events? (describe in the notes section)	N/A	—
2-3	Indicate what information is used to identify individual events recorded in the audit log:		
2-3.1	**User** ID	Yes	—
2-3.2	Date/time	Yes	—
AUDT notes:	1. Remote Service Logins are logged using operating system auditing.		
3	AUTHORIZATION (AUTH) The ability of the **device** to determine the authorization of **users**.		
3-1	Can the **device** prevent access by unauthorized **users** through **user** login requirements or other mechanism?	Yes	—

3-2	Can **users** be assigned different privilege levels within an application based on 'roles' (e.g., guests, regular **users**, power **users**, administrators, etc.)?	Yes	—
3-3	Can the **device** owner/**operator** obtain unrestricted administrative privileges (e.g., access operating system or application via local root or admin account)?	No	1
AUTH notes:	1. Due to data distribution in different services, a local root access does not allow access to PHI via the application. 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.		
Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.		Yes, No, N/A, or See Note	Note #
4	CONFIGURATION OF SECURITY FEATURES (CNFS) The ability to configure/re-configure **device security capabilities** to meet **users'** needs.		
4-1	Can the **device** owner/**operator** reconfigure product **security capabilities**?	Yes	1
CNFS notes:	1. Configuration changes are subject to audit logging.		
5	CYBER SECURITY PRODUCT UPGRADES (CSUP) The ability of on-site service staff, remote service staff, or authorized customer staff to install/upgrade **device**'s security patches.		
5-1	Can relevant OS and **device** security patches be applied to the **device** as they become available?	Yes	—
5-1.1	Can security patches or other software be installed remotely?	Yes	1
CSUP notes:	1. Siemens Remote Service infrastructure provides secure means for downloading security patches and application-specific updates. Additionally, application-specific security patches can be provided by a software repository that can be manually propagated. 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.		
6	HEALTH DATA DE-IDENTIFICATION (DIDT) The ability of the **device** to directly remove information that allows identification of a person.		
6-1	Does the **device** provide an integral capability to de-identify **private data**?	No	1
DIDT notes:	1. 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. The Document Registry Service can be configured to discard any demographic data (PHI) received even if contained in document metadata.		
7	DATA BACKUP AND DISASTER RECOVERY (DTBK) The ability to recover after damage or destruction of **device** data, hardware, or software.		
7-1	Does the **device** have an integral data backup capability (i.e., backup to remote storage or **removable media** such as tape, disk)?	No	1
DTBK notes:	1. 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.		
8	EMERGENCY ACCESS (EMRG) The ability of **device users** to access **private data** in case of an emergency situation that requires immediate access to stored **private data**.		

8-1	Does the **device** incorporate an **emergency access** (“break-glass”) feature?	Yes	1
EMRG notes:	1. System provides special PurposeOfUse element in SAML Token to indicate emergency access. Emergency access requires successful authentication and is subject to audit logging.		
9	HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU) How the **device** ensures that data processed by the **device** has not been altered or destroyed in an unauthorized manner and is from the originator.		
9-1	Does the **device** ensure the integrity of stored data with implicit or explicit error detection/correction technology?	Yes	1
IGAU notes:	1. Repository persistence backup supports integrity checks based on cryptographic checksums.		
10	MALWARE DETECTION/PROTECTION (MLDP) The ability of the **device** to effectively prevent, detect and remove malicious software (**malware**).		
10-1	Does the **device** support the use of **anti-malware** software (or other **anti-malware** mechanism)?	Yes	—
10-1.1	Can the **user** independently re-configure **anti-malware** settings?	Yes	1
10-1.2	Does notification of **malware** detection occur in the **device** user interface?	No	—
10-1.3	Can only manufacturer-authorized persons repair systems when **malware** has been detected?	No	—
10-2	Can the **device** owner install or update **anti-virus software**?	Yes	—
10-3	Can the **device** owner/**operator** (technically/physically) update virus definitions on manufacturer-installed **anti-virus software**?	Yes	—
MLDP notes:	1. Anti-malware software is not included and not integrated in the device. The operation of anti-malware software and mechanisms should be done by the customer. Anti-virus software can be installed by the device owner. However, it is recommended to update anti-virus software in coordination with the device manufacturer. Malware detection can be integrated on a per-document basis in the submission and retrieval workflow. This allows documents to be scanned for malware prior to persistence in the repository as well as prior to display in web applications.		
11	NODE AUTHENTICATION (NAUT) The ability of the **device** to authenticate communication partners/nodes.		
11-1	Does the **device** provide/support any means of node authentication that ensures 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. System is compliant with the strict requirements of IHE Audit Trail and Node Authentication Profile – Secure Node, which implies mutual node authentication between client and service based on client and server certificates and TLS 1.2 encryption.		
12	PERSON AUTHENTICATION (PAUT) 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?	Yes	—
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?	Yes	—

PAUT notes:	
13	PHYSICAL LOCKS (PLOK) Physical locks can prevent unauthorized **users** with physical access to the **device** from compromising the integrity and confidentiality of **private data** stored on the **device** or on **removable media**.

13-1	Are all **device** components maintaining **private data** (other than **removable media**) physically secure (i.e., cannot remove without tools)?	Yes	1

PLOK notes:	1. Hardware server rack should be locked against unauthorized removal by the customer.
14	ROADMAP FOR THIRD-PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP) Manufacturer's plans for security support of 3rd-party components within **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 of other third-party applications provided by the manufacturer available?	Yes	2

RDMP notes:	1. Application server uses Red Hat Enterprise Linux 7 64-Bit. Clients are browser-based and thus independent from the operating system. 2. A complete list of third-party software and libraries is included in the Release Notes of the product.
15	SYSTEM AND APPLICATION HARDENING (SAHD) The **device**'s resistance to cyber attacks and **malware**.

15-1	Does the **device** employ any hardening measures? Please indicate in the notes the level of conformance to any industry-recognized hardening standards.	Yes	—
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** (i.e., a source other than an internal drive or memory component)?	No	—
15-11	Can software or hardware not authorized by the **device** manufacturer be installed on the **device** without the use of tools?	Yes	1

SAHD notes:	1. The manufacturer does not restrict additional software that may be installed by the customer.
16	SECURITY GUIDANCE (SGUD) The availability of security guidance for **operator** and administrator of the system and manufacturer sales and service.

16-1	Are security-related features documented for the **device user**?	Yes	—
16-2	Are instructions available for **device**/media sanitization (i.e., instructions for how to achieve the permanent deletion of personal or other sensitive data)?	Yes	—

SGUD notes:	
17	HEALTH DATA STORAGE CONFIDENTIALITY (STCF) The ability of the **device** to ensure unauthorized access does not compromise the integrity and confidentiality of **private data** stored on **device** or **removable media**.

17-1	Can the **device** encrypt data at rest?	Yes	1

STCF notes:	1. The vendor encourages customers to apply storage and database encryption.
18	TRANSMISSION CONFIDENTIALITY (TXCF) The ability of the **device** to ensure the confidentiality of transmitted **private data**.

18-1	Can **private data** be transmitted only via a point-to-point dedicated cable?	No	—
18-2	Is **private data** encrypted prior to transmission via a network or **removable media**? (If yes, indicate in the notes which encryption standard is implemented.)	Yes	—
18-3	Is **private data** transmission restricted to a fixed list of network destinations?	Yes	—

TXCF notes:	

19	TRANSMISSION INTEGRITY (TXIG) The ability of the **device** to ensure the integrity of transmitted **private data**.		
19-1	Does the **device** support any mechanism intended to ensure data is not modified during transmission? (If yes, describe in the notes section how this is achieved.)	Yes	1
TXIG notes:	1. System solely uses TLS 1.2-encrypted communication paths, which implies authenticity of transmitted data.		
20	OTHER SECURITY CONSIDERATIONS (OTHR) Additional security considerations/notes regarding **medical device** security.		
20-1	Can the **device** be serviced remotely?	Yes	—
20-2	Can the **device** restrict remote access to/from specified devices or **users** or network locations (e.g., specific IP addresses)?	Yes	1
20-2.1	Can the **device** be configured to require the local **user** to accept or initiate remote access?	Yes	2
OTHR notes:	1. Can be handled by specific firewall settings. Remote service source addresses are available. 2. Acceptance of remote service request depends on the local network infrastructure. Acceptance of incoming service requests should be handled by the underlying network security infrastructure that allows remote connections to specific machines.		

4.15 Abbreviations

Table 5: List of Technical Abbreviations

ADT	Admit, Discharge & Transfer (HL7)
ATNA	Audit Trail and Node Authentication
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
LDAP	Lightweight Directory Access Protocol
MDM	Medical Document Management
MDS^2	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
WSS	WebSocket Secure

XACML	Extensible Access Control Markup Language
XDS	Direct Save Protocol
XML	Extensible Markup Language
XSS	Cross-Site Scripting

4.16 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.

4.17 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.

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