eHealth solutions
Product and Solution Security Statement

A high level of data security and patient safety is a key success factor for end-user acceptance and trust in electronic health records. Thus Siemens Healthineers eHealth solutions ensures continuous product and solution security, as well as patient safety throughout the entire software and deployment lifecycle.

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

We are confident that those requirements can be better addressed by providing evidence of a continuous product and solution security process rather than by demonstrating privacy certificates. This process encompasses the following patient safety and data security measures:

- The software is developed according to a stringent development processes and meets Siemens' requirements, as well as additional strict quality requirements including risk management, design approval with specific focus on security and periodic code reviews.
- The processes of software development, quality management and change management are EN ISO 13485 and EN ISO 9001 certified. This encompasses an expansive risk management process for new and changed requirements. Risk analysis and identification of control measures is carried out with particular focus on data security and patient safety.
- The legal manufacturer, the Siemens Healthineers company ITH icoserve is certified to the strict criteria of EuroREC (http://www.eurorec.org) for usability and privacy for electronic health records.
- eHealth Solutions have undertaken an intensive security analysis carried out by the Department of Computer Science of the Leopold-Franzens-University 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 below) 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 fulfilling 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 has undertaken security audits carried out in the scope of the Austrian Electronic Health Record (ELGA).
- Portal applications are based on the Liferay Enterprise Portal Solution. "Liferay follows The Open Web Application Security Project **OWASP Top 10** and CWE/SANS Top 25 lists to ensure that Liferay Portal is as secure as possible. Following these recommendations protects the portal against known kinds of attacks and security vulnerabilities" See https://dev.liferay.com/discover/deployment/-/knowledge_base/7-0/liferay-portal-security-overview . Furthermore, the Liferay development cycle follows a detailed Security Policy. https://www.liferay.com/security-statement. Portal applications running on Liferay directly benefit from these commitments and can therefore be considered as highly robust against the OWASP top 10 security flaws. Additionally sense applications are developed with awareness of the OWASP top 10 security issues, as well as further security patterns. Constant training of developers with particular focus on those patterns allows the development of sense applications that provide robust designs against the OWAS 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 leading edge security measures are followed and upcoming risks are identified and mitigated instantly.
- In scope of an information security management system (ISMS) 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.

Please note:

Effective security of a particular eHealth projects' implementation mainly depends on local security configurations of the deployment site. This includes hardware, network topology and firewall rules, encrypted connections with primary systems, operating system, databases, as well as the currently active configuration of the eHealth software, including authentication and access control policies.

To reflect the local and country-specific characteristics of the configuration we recommend external security audits by independent organizations to be carried out at the end of the deployment phase directly before go-live.

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

eHealth solution is a product of ITH icoserve technology for healthcare GmbH, Innsbruck,Austria.
eHealth solution is not available in all countries. Please contact your local Siemens sales representative for the most current information.