Security
Concept
version 10.0

Smart Remote Services

Your smart connection to digital services

siemens-healthineers.com/srs

SIEMENS Healthineers

Content

"The support we receive through SRS provides us with a fast and personalized answer to questions or issues [...]. By having remote access to our server, the syngo supporters (Remote Support Engineers) are really efficient, and can access our workstations, take the control, in order to guide us step by step, for every demand that we have, so we never feel abandoned."

Nullam Jeremy Brachet
MRI Technician, IRM Lyon Nord, Lyon, France.

Smart Remote Services (SRS)

Your smart connection to digital services

High availability, diagnostic confidence, and smooth running operations are key to meeting your performance requirements. At the same time, keeping equipment state of the art is a top priority to protect equipment and patient data. In light of these needs, we systematically focus on being proactive to keep you on the path to success. Smart Remote Services (SRS) is a fast, secured, and powerful data link connecting your medical equipment to our experts, who provide you with proactive and interactive services that support you in your daily routine and speed up your running operations.
The SRS connection gives you access to our wealth of Remote Services which enable you to:

- **improve diagnostic and clinical outcomes** through context-specific interaction and immediate Remote Application Support;
- **enhance performance and functionalities** through regular Remote Software Updates, keeping your system up to date at all times;
- **increase system uptime** through real-time remote system monitoring and the proactive scheduling of service events.

This Security Concept describes the measures we at Siemens Healthineers have undertaken, in both technical support and clinical application areas, to securely transfer device data and protect patient data when performing SRS-based services on your medical devices. The concept is to be used in conjunction with all products for which SRS is offered.

Siemens Healthineers is one of the first manufacturers of medical devices worldwide to implement an internationally valid Information Security Management System (ISMS) for the remote service of medical devices and software systems. The system has been certified by TÜV Süd in Germany according to the international standard ISO/IEC 27001, 2. Edition. The ISO/IEC 27001 certificate and the associated Statement of Applicability (list of controls) is available to all customers.

1 Security measures in our remote service delivery process

Smart Remote Services is our channel to remotely respond to your requests for reactive and interactive services (Remote Technical and Application Support) and to provide you with data-driven proactive services. Due to the varied nature of the services we deliver through Smart Remote Services, we follow different approaches to protect your business, whether these services are delivered by employees of Siemens Healthineers or by authorized Business Partners.

a Remote Technical Support

Our incident handling process follows a three-step escalation approach where we use Smart Remote Services as a direct channel to provide remote troubleshooting and expert support for our products.

Our engineers at the Customer Care Center will react upon your request for support and access your system remotely for early diagnosis and troubleshooting. In addition, our Remote Services Center specialists may also remotely access your system to provide support on issues requiring second-level attention. For IT systems—such as PACS or advanced postprocessing systems—first-level support is provided by our Remote Services Center specialists.

Our products that run syngo®[1] applications software include mechanisms to mask any patient data before transferring it to the Customer Care Center conducting remote troubleshooting. The most recent software versions[2] also have the ability to define which users have access to which data within the device (see section 2). This leaves the decision of whether to grant access to a Service Engineer or your own employees in your hands.

For products that do not run *syngo*, a granular access control to the data is not implemented. In these cases, we rely on our organizational measures and our Smart Remote Services infrastructure (see section 4) to safeguard your data.

b Remote Application Support

In order to support your clinical staff with application questions, our Customer Care Center or Remote Services Center Application Specialists can use Smart Remote Services to mirror your system display and remotely guide the user with remote desktop management tools.

Our products explicitly require you to grant this remote access and allow you to track and terminate access at any point during the course of the online support session.

Most of the in vitro products offer an extra layer of security by masking any Protected Health Information (PHI) when a remote session is detected to mitigate the risk of having PHI visible outside your institution. Further details can be found in the Security White Paper for the respective medical device.

c Proactive monitoring services

Certain proactive services require your device to regularly send a predefined set of data to our Remote Service Centers. This includes system logs, as well as statistical and reliability data, such as the number of scans performed and how often the system has restarted.

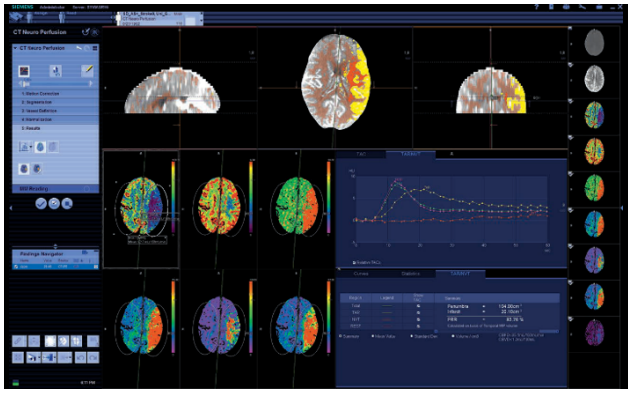


Figure 1: *syngo* user interface: Making Patient Health Information anonymous

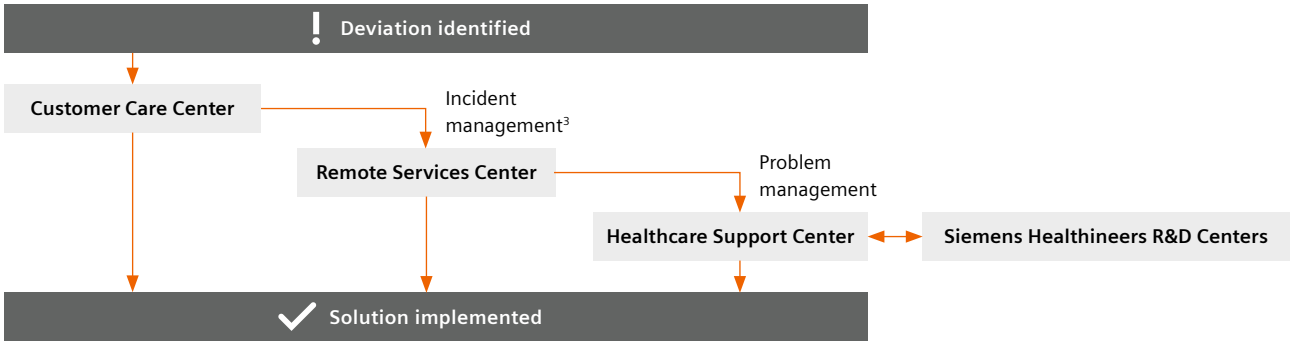
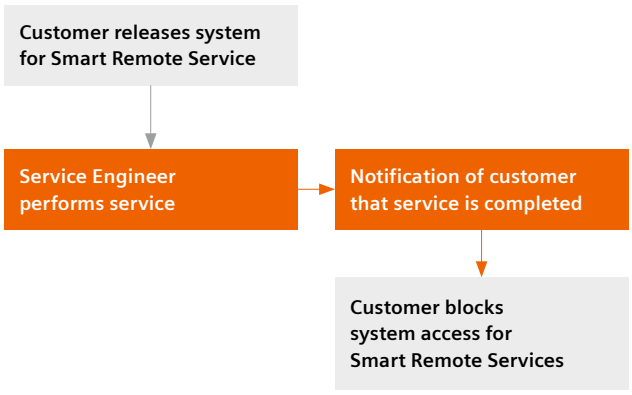


Figure 2: Siemens Healthineers escalation process for handling service calls

[1] *syngo® is a registered trademark of Siemens Healthcare GmbH.*
[2] *Information regarding the software version on your system may be obtained from your representative of Siemens Healthineers.*
[3] *Depending on the product line, incident management can be directly handled at our Remote Services Center.*



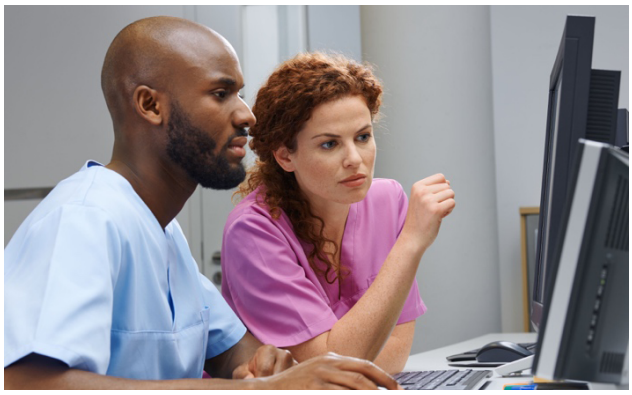


Figure 3: Workflow of SRS activities at "no access" level

2 SRS security measures in our applications software

a SRS security measures in our in vivo products based on *syngo* applications software

Our products that run *syngo* applications software[4] can be configured with the following features to support data security throughout the whole remote interaction.

Session control
You can define the level of access granted to a system running our *syngo* applications software. Every application support session requires a one-time session password. This allows you to decide on a case-by-case basis whether to share your monitor with our expert. Once the issue is resolved, the connection is terminated. Accessing your systems without your authorization is not possible.

When establishing a remote service connection, you can choose between four access levels:

- **No access**
  You provide access only on a case-by-case basis to perform the approved task. Patient examinations can still be conducted.
- **Limited/Restricted access**
  For a predefined time period, the authorized Service Engineer from Siemens Healthineers has access to a subset of service functionalities that do not interfere with ongoing examinations.
- **Permanent limited access**
  The authorized Service Engineer from Siemens Healthineers has access to a subset of service functionalities that do not interfere with ongoing examinations. There is no time limitation on this access.
- **Full access**
  The authorized Service Engineer has full access to all service functionalities. Patient examinations are not possible while remote servicing is being performed.

These access levels solely determine the time period for which you wish to grant service access to your system and the degree of access. In each session, you have control over granting or revoking access rights at all times.

While permanent limited access is the most frequently chosen access level, you can always opt for the "no access" level. Figure 3 shows the workflow of a remote service task at this level.

Note: The session control described above is not applicable to server-based IT systems, such as PACS or advanced postprocessing workstations. Remote access to such systems can be established without direct interaction with the end users, as they do not necessarily affect a dedicated workplace.

[4] *Generally includes our diagnostics imaging modalities, and excludes server-based systems such as syngo.via and syngo.plaza*

Access control
As a prerequisite for every service activity, you must expressly grant SRS access to your system. Adjusting measurement parameters is only technically possible during an application support session and with your authorization. After a fixed period of idle time, the SRS session on your system is automatically terminated.

Password protection
When you allow access to your system, the Service Engineer/Application Expert must be authenticated on your system with a valid time-dependent password before being allowed to log onto the system.

For IT systems integrated into your IT domain, it is possible to adapt the system password policies and security measures to your environment, as long as they do not impact system functionality.

Four-eye principle
During every remote session, your system screen indicates (in the bottom right-hand corner) that remote service activities are in progress. Nevertheless, our Service Engineers/Application Experts will explain in a voice call what actions they are conducting. If you decide to terminate the session, all service programs currently running will immediately be shut down in a controlled manner, with no impact on the continued safe operation of the system.

Email notification of remote connections
Upon your request, we can enable an email service providing the connection details of each remote connection to an email address of your choice. This email can be followed up after each session with a second message containing further information on the activities performed. These emails are sent from the SRS DMZ (see section 4), and not from the medical systems themselves.

b SRS security measures for our laboratory diagnostics equipment and software

Our laboratory diagnostics instruments are enabled for Remote Monitoring and support through Smart Remote Services by the following three elements:

- Proprietary software protocol on the instrument to facilitate communication with the SRS Gateway (ATELLICA CM)
- Smart Remote Services Gateway software (residing on the SRS Gateway) initiating and maintaining a consistent connection to the Smart Remote Services infrastructure through the virtual network adapter via the site connection to the Internet
- Smart Remote Services infrastructure

The SRS Gateway connects to the Smart Remote Services infrastructure through an Internet connection supporting HTTPS requests on outbound port 443. Smart Remote Services provides both ongoing Remote Monitoring of connected devices from Siemens Healthineers and as-needed remote desktop support.

Access control
Remote access is restricted to authorized personnel and assets of Siemens Healthineers with appropriate authentication credentials.

On both the instruments and SRS Gateway there are service user accounts that are required to effectively manage the functions of the product. When issues arise, authorized service personnel from Siemens Healthineers may need to access the instrument desktop. These service personnel will log onto the Smart Remote Services infrastructure and request a live connection to the instrument. All interactions between service personnel from Siemens Healthineers and the hospital or laboratory's connected instruments are through the SRS application and managed by the Atellica® Connectivity Manager (ACM), which prevents your devices from being directly exposed to the outside network. All user and system interactions conducted by Siemens Healthineers are recorded and available for audit.

Session control
You can define the level of access available to remote users through the SRS Gateway GUI. The SRS Gateway GUI then provides this level of control to all connected instruments. You can benefit from full control over file uploads, downloads, and remote desktop access to your devices. You can grant or deny access to remote sessions, software updates, and applications. If a computer issue arises, you can request a remote access session with authorized service personnel from Siemens Healthineers only. There are additional service user accounts that are required to effectively manage the functions of the product. These may not be removed or modified.

SRS remote desktop sessions are initiated on an ad hoc basis and are usually related to investigating equipment issues. Authorized service personnel from Siemens Healthineers who are logged onto the Smart Remote Services application can request remote access to an instrument or SRS Gateway. After the request is initiated, you should accept it at the instrument within 30 seconds or the request times out. If access is granted, all remote activities will be visible on the instrument monitor. The Smart Remote Services infrastructure logs the remote connections and file transfers. In all cases, your local system operator must accept the remote desktop session to allow the remote user to continue.

Network control
SRS supports the following:

- Static IP addressing and DHCP assignment
- NTLM authentication when using an ISA server as a proxy communication channel, via standard and authenticating proxy servers, as required

Data transfer
All communication between the Smart Remote Services infrastructure and the local SRS Gateway (Atellica CM) is encrypted by design. The communication between the local SRS Gateway and instruments can be encrypted for some instruments; for specific details, please refer to the Security White Paper of your medical device from Siemens Healthineers.

Remote Monitoring is facilitated by the transfer of data from the instrument to the Smart Remote Services infrastructure via the SRS Gateway. Depending on the instrument and the dataset affected, the transfer to the Smart Remote Services infrastructure may be initiated either by the instrument itself or by the service personnel of Siemens Healthineers logged onto the SRS application.

3 Security measures for information in transit

To securely transport data between your environment and the Smart Remote Services infrastructure we employ a secured, encrypted connection. If you also opt to route all network traffic through your own firewall you will obtain full control over your communication.

The in vitro medical devices offer Internet-Based Connectivity (IBC) technology to create a virtual private connection (VPN). In addition to IBC, the in vivo medical devices offer IPsec and WebSocket/TLS connectivity technologies to create the VPN connection.

Security measures for IPsec connectivity

Our Smart Remote Services use an IPsec solution to connect the two environments.

If you do not have a VPN endpoint, Siemens Healthineers may provide you with the VPN endpoint device required for the SRS connection. We regularly monitor security advisories and remotely update the software of these VPN endpoints if required. We track all configuration changes in our configuration management database and update the field devices accordingly.

If you already have your own solution, our technicians can help you to implement the necessary parameters for the connection. These parameters must then be safeguarded against unauthorized changes.

Our VPN backend endpoints are Cisco© routers. In the event of incompatibilities when setting up the connection, please contact your local representative from Siemens Healthineers.

We have put a number of security measures in place to protect the connection:

Access Control Lists
Access Control Lists (ACLs) on your service router provide a similar function to firewalls: they only allow data traffic to and from known IP addresses. The data traffic is routed through the reverse proxy in the SRS DMZ to the system (see section 4). They also prevent access by Siemens Healthineers to other parts of your network and access by unauthorized parties.

IP Security Protocol suite
To prevent network sniffing and data tampering, Siemens Healthineers uses the established IP Security Protocol (IPsec) (suite) with pre-shared secret keys for encrypted and authenticated data transmission. Pre-shared secret keys consist of an arbitrary string of random characters.

The Internet Security Association and Key Management Protocol (ISAKMP) is used to exchange encryption key information. Due to backward compatibility with some legacy connections, we still need to support parameters such as SHA1, MD5, and 3DES in consultation with some customers. Nevertheless, we are diligently working with them on migrating the current configuration to the newly recommended parameters.

For new connections, we recommend the following minimum configuration parameters:

Authentication/integrity	SHA-256
Encryption	AES-256/AES-GCM-256
Key exchange	DH-group-16 (4096 bit)

To enhance data privacy while protecting data integrity we also support higher levels of encryption through, e.g., authentication methods SHA-384 or SHA-512, Diffie-Hellman Groups (19-256 bit ec, 20-384 bit ec, 21-521 bit ec, 24-2048/256 bit) for key exchange security.

Security measures for Internet-Based Connectivity

The SRS Security Concept is based on Internet-Based Connectivity (IBC) which uses Transport Layer Security (TLS) technology. This technology provides a secured and private communication channel for data exchange between the system and the SRS DMZ by establishing a direct encrypted network tunnel. This supports data protection and prevents virus infection from unauthorized third parties during an SRS connection.

The certificate is issued by the SRS private Certificate Authority located in the SRS backend. The certificate is not stored in the Cert Store (i.e., Cert Manager), but rather delivered and stored in a file within the installation directory of the SSL VPN client. For further details, please refer to the Security White Paper from the medical device (in vivo) or ACM gateway (in vitro), or contact your local representative from Siemens Healthineers.

Internet-Based Connectivity which uses TLS is increasingly being recognized throughout the industry as a highly viable and economical solution for remote access. Internet-Based Connectivity allows your medical devices to be connected to the Smart Remote Services infrastructure based on an Internet connection, with no additional hardware or network requirements, while at the same time safeguarding your data and offering greater system mobility.

Security measures for WebSocket/TLS connectivity

WebSocket is a connection technology recently introduced by SRS that will gradually replace IBC in the future. This technology provides a full duplex communication channel via a single TCP connection using port 443. As is the case with IPsec and IBC, WebSocket provides a secured, encrypted bidirectional communication channel between the medical device and the SRS DMZ, where the client (located on the medical device) establishes the initial connection with the Smart Remote Services infrastructure.

Whenever provided by the medical device, WebSocket will be the preferred technology to connect your systems to SRS, as enables enhanced security and improved service delivery.

Connectivity options for Websocket/TLS connectivity

1. **Direct connectivity via customer Internet access**
   Medical device connects directly via customer Internet access to dedicated SRS cloud or SRS DMZ endpoints.
2. **Centralized connectivity via customer proxy**
   Medical device connects directly via the customer proxy to dedicated SRS cloud or SRS DMZ endpoints.
3. **Centralized connectivity via SHS VPN endpoint**
   Medical device connects directly via VPN endpoint provided by Siemens Healthineers to dedicated SRS cloud SRS DMZ endpoints.

Transmission from your systems to the Smart Remote Services infrastructure

Data exchange via the SRS connection is triggered through two different mechanisms. Please note, the data volume transferred is highly dependent on the product itself and the phase of the product's life cycle and can therefore generally not be quantified.

User-initiated transfers

The data transfer is remotely "pulled" from the system by an authorized Service Engineer, or a data "push" is scheduled to solve a specific issue on the system.

Data "pulls" are necessary when our Customer Care Center service personnel first try to troubleshoot a reported issue by using the log data stored locally on the medical device. If this is not possible and further support from experts is required, the Remote Service Engineer can initiate a data transfer to the SRS backend. This data is accessible to the specialists at the Customer Care Center, Remote Service Center, and Headquarters Support Center, including the product R&D team. In specific error cases, it might also be necessary to pull data which includes PHI/PII (e.g., body height and weight of a patient in MRT studies) in addition to the technical data. This data will only be accessed and used for solving the issue encountered. The service personnel are regularly trained and reminded of data privacy measures and how to handle data that potentially contains PHI/PII.

System-initiated transfers

Automatic data "push" transfers are initiated at regular, predefined times. For in vivo devices, the transfers are done via file transfer and in a limited number of systems, through emails from the system to the SRS backend. For in vitro devices, transfers are done using a proprietary protocol. Further details of the technical data transmitted and their intended use are described in the respective Remote Connection Terms and Conditions, which should be agreed upon in advance.

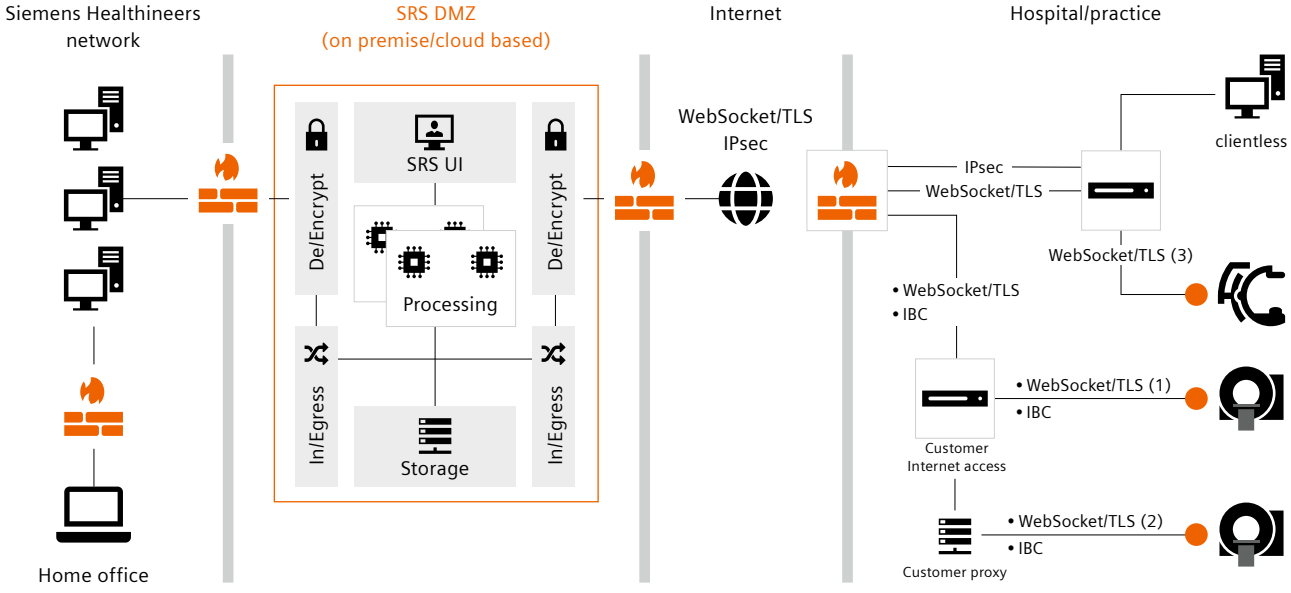


Figure 4: Security infrastructure of SRS

Firewall *SHS VPN endpoint device* *SRS client*

4 Security measures in our Smart Remote Services infrastructure

Our Smart Remote Services rely on the secured operation of our SRS connection and the SRS Demilitarized Zone (SRS DMZ) (see section 4c) between the Siemens Healthineers intranet and the Internet. The following measures are in place to enable data protection in our Smart Remote Services infrastructure.

a Authentication and authorization

The central maintenance platform (Smart Remote Services infrastructure) used by the Customer Care Center is hosted in an isolated segment of the company intranet. Access is restricted via single sign-on two-factor authentication. The first factor is a combination of PKI and username/password and the second is a one-time password (OTP) via mobile app/SMS or email.

The granularity of our authorization concept allows us to define which users can access which systems (need-to-know basis). In practice, this means that only authorized service personnel who need to access a system to provide support, and who are not explicitly prevented from doing so, can access such systems to perform the support tasks they are authorized for.

b Remote access logging

We record every instance of direct access to your system in the Smart Remote Services infrastructure and apply a time stamp and a unique user identification to the Service Engineer/Application Expert responsible. This information will be stored for up to six years, unless applicable laws and regulations require a different retention period, and access to this information, to the extent available, can be provided upon request.

c SRS Demilitarized Zone

Between your network and Siemens Healthineers intranet, we have established a SRS Demilitarized Zone (SRS DMZ) that prevents direct connectivity between the two environments. There are multiple SRS DMZ locations across the world, either on-premise or cloud-based, to provide a reliable connection, while reducing latency of the remote communication at the same time. Access to your medical equipment is only permitted to authorized users via the SRS DMZ and all sessions are tracked for audit purposes. This architecture is designed to mitigate the risk of unauthorized network access through a so-called reverse proxy server, in order to protect from the transmission of malware between our respective networks.

d Protected Smart Remote Services infrastructure

Smart Remote Services operates an on-premise or cloud-based infrastructure according to the Information Security guidelines of Siemens Healthineers. The effectiveness of the protection measures is audited regularly to enable the Smart Remote Services infrastructure to operate using up-to-date technology.

e Organizational measures

Siemens Healthineers is one of the first manufacturers of medical devices worldwide to implement an Information Security Management System (ISMS) for the remote service of medical devices and software systems. This has been certified by TÜV Süd in Germany according to the international standard DIN EN ISO/IEC 27001, 2. Edition.

In addition, Siemens Healthineers operates a Privacy Information Management System based on the ISO/IEC 27701:2019 standard.

Our Service Engineers and Application Experts have been trained in and are committed to data privacy and security issues. Siemens Healthineers hosts an electronic record of these service employees and their corresponding access rights.

You can find more details on topics related to data privacy in the Smart Remote Services Data Privacy White Paper.

5 Protection against malicious attacks

All the measures in this Security Concept are designed to provide holistic end-to-end protection for your systems and your environment, and particularly to minimize the risks from the following specific threats.

a Malware infections

The continuous monitoring and maintenance of the SRS backend contributes to keeping the connection between your medical devices and the SRS backend secured. As long as Internet access is used for SRS purposes only, and the product is operated according to its Security White Paper, virus infections are unlikely.

b Malicious email traffic

Certain types of in vivo medical devices send emails to the Smart Remote Services infrastructure. These emails are sent from your system to our SRS DMZ.

Emails sent from your system to the SRS DMZ are forwarded to the appropriate email server of Siemens Healthineers and then relayed to the recipient. These could be email addresses from Siemens Healthineers or from your own IT department. Each recipient address has to be whitelisted before an email is allowed to be relayed. No emails are sent from the SRS DMZ to the medical device.

In vitro medical devices do not send emails to our SRS DMZ.

c Cross-system infections

Cross infection between the Service Engineer workplace and your system is unlikely, because there is no direct IP routing between them (see the reverse proxy function in section 3).

6 How to support your equipment further

Despite our firm commitment to cybersecurity, the nature of our different products may require your involvement in helping to run them securely. All our equipment and software-only products are released with a Security White Paper and/or a Manufacturer Disclosure Statement for Medical Product Security (MDS2). In these documents, you will find further information on the security controls implemented on the medical device, and the additional factors you need to consider when setting up your IT infrastructure while carefully following the principle of security, with strict security policies in all IT layers. This means that all network devices, operating systems, application software, office and clinical IT devices have their own adequate security controls to protect from flaws that may have been overlooked in other IT elements. Please contact your Customer Services representative from Siemens Healthineers for the Security White Paper of your medical device from Siemens Healthineers.

In addition, SRS is our fast channel to deliver third-party security patches when required. Therefore, unless otherwise stated, it is highly recommended that you actively stay connected to SRS in situations where new vulnerabilities affecting your medical devices are disclosed.

The product/features and/or service offerings (here mentioned) are not commercially available in all countries and/or for all modalities.

If the services are not marketed in countries due to regulatory or other reasons, the service offering cannot be guaranteed.

Please contact your local Siemens Healthineers organization for further details (including technical prerequisites that apply to certain service offerings).

Prerequisites:
Stable SRS connection with adequate bandwidth

Siemens Healthineers Headquarters
Siemens Healthineers AG
Siemensstr. 3
91301 Forchheim, Germany
Phone: +49 9191 18-0
siemens-healthineers.com

Published by Siemens Healthineers AG · 13983 0224 Online ·