Security
Concept
Version 8.1

Smart Remote Services

System support. Whenever you need us.

siemens-healthineers.com

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 secure connection to support in digitalizing healthcare

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

- **Optimize diagnostic and clinical outcomes –** through context-specific interaction and immediate remote application support
- **Enhance performance and functionalities –** through regular remote software updates enabling your system to be always up to date
- **Maximize 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 undertaken to protect patient data when performing SRS-based services, in both technical support and clinical application areas, on our medical devices. It is 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 a software systems. This has been certified by TÜV Süd in Germany according to the international standard ISO 27001. The ISO 27001 Certificate and the associated Statement of Applicability (list of controls) is available to every customer.

1. Security measures in our remote service delivery process

Our Smart Remote Services is our channel to remotely respond to your requests for support and to provide you with data driven proactive services. Due to the different nature of the services we deliver through Smart Remote Services we follow different approaches to protect your data.

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.

Within this process, our engineers at the Customer Care Center access your system remotely for early diagnosis and troubleshooting. In addition, our Remote Services Center specialists may also remotely access your system to support issues requiring second level attention. For IT systems – like PACS or advanced post-processing systems – the first level is provided by our Remote Services Center specialists.

Our products running *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 allow to define which users have access to which data within the device (see section 2). This leaves the decision to grant access to a Service engineer or your own employees in your hands.

Products not running *syngo* are typically PACS workplaces managing databases. For these products a granular access control mechanism to the data is not technically implemented. In those cases, we rely on our organizational measures and our IT 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 our Remote Services Center application specialists can use Smart Remote Services to mirror your systems 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 the access at any point through the course of the online support session.

c. Proactive monitoring services
Certain proactive services require your device to regularly send a predefined set of data to our Service Centers. This includes system logs, statistical and reliability data, such as the number of scans performed and how often the system has restarted. We do not gather up patient data as part of our proactive services.

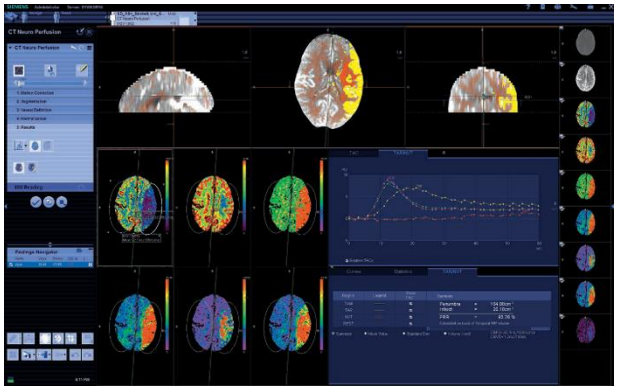


Figure 1*: syngo* user interface: Making patient health information anonymous

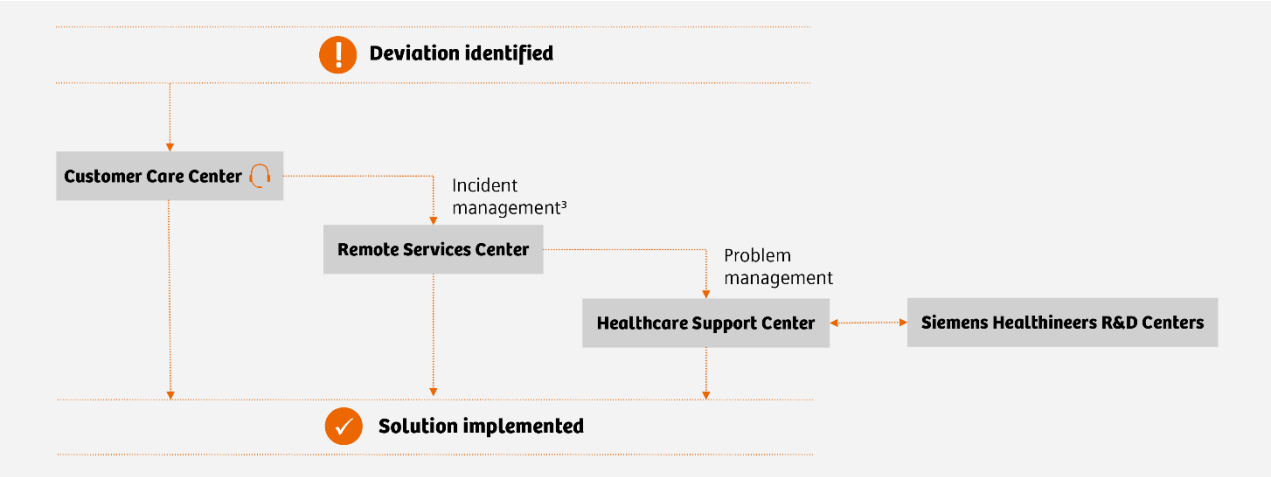
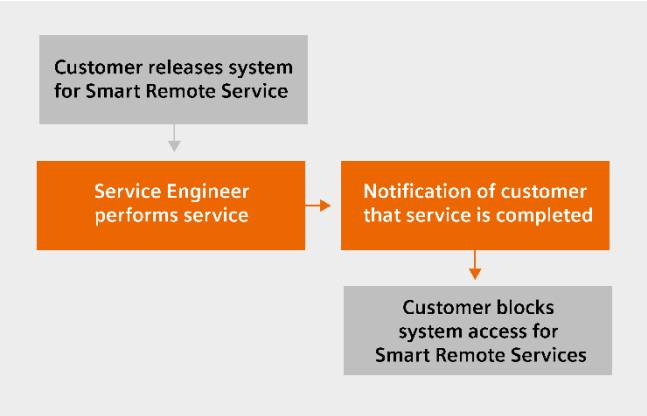


Figure 2: Escalation process for handling service calls

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



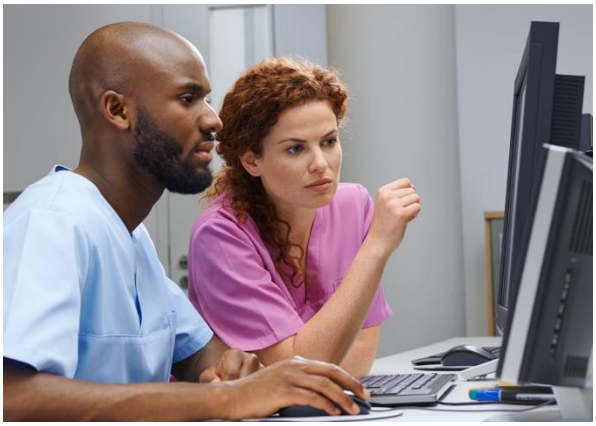


Figure 3: Workflow of SRS activities at "no access" level

2. SRS Security measures in our applications software

a. SRS Security measures in our *syngo* applications software

Our products running *syngo* applications software[3)] can count with the following features to support data security through the whole remote interaction.

Session control

The level of access granted to a system running our *syngo* applications software is determined entirely by the customer. Every application support session requires an ad-hoc session password. This allows you decide whether you share your monitor with our expert on a case-by-case basis. After solving the issue, 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 task approved. Patient examinations using the system can still be conducted.

- **Limited access**

During a predefined timeframe the authorized Siemens Healthineers Service Engineer has access to a subset of system functionalities that do not interfere with ongoing examinations.

- **Permanent limited access**

The authorized Siemens Healthineers Service Engineer has access without time limitations to a subset of system functionalities that do not interfere with ongoing examinations.

- **Full access**

The authorized Service Engineer has full access to your system. Patient examinations are not possible while remote servicing is being performed.

These access levels alone determine the degree and time frame for which you wish to grant access to your system. At all times you have the control over the session to grant or revoke access rights. Regardless of what access level you choose, transmission of patient data is automatically blocked out.

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.

Remark: the session control described above is not applicable to server-based IT systems, like PACS or advanced post-processing workstations. Remote access for such systems can be established without direct interaction with the end-users, as they don't necessarily affect a dedicated workplace.

3) 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 the system. Adjusting measurement parameters is technically possible only during application support and with your authorization. After a fixed period of idle time the SRS session at your system is automatically terminated.

Password protection
When you allow access to your system, the Service Engineer/Application Expert must be authenticated at your system with a time-dependent password before being allowed to switch the system to service mode. Siemens Healthineers uses state-of-the-art password policies for our service engineers, including the regular update of passwords.

For IT systems which are integrated under your IT domain it is possible to adapt the system password policies and security measures of your environment, if they don't impact system functionality.

Four eye principle
During every remote session your system screen visually displays that remote service activities are in progress. Our Service Engineers/Application Experts shall nevertheless explain by phone what actions they are conducting. If you decide to terminate the session, all service programs currently running are immediately shut down in a controlled manner, with no impact to the continued safe operation of the system.

E-mail notification of remote connections
We can enable an e-mail service providing the connection details of each remote connection to your designated technical, clinical, and/or management staff. This e-mail can be complemented by a second message with further information on the activities performed after every session. These emails are sent from the SRS DMZ, and not from the medical systems themselves.

b. SRS Security measures in our Laboratory diagnostics equipment and software

The Atellica Connectivity Manager and the *syngo* Laboratory Connectivity Manager systems use Smart Remote Services (SRS) for remote monitoring and support. SRS functionality is supported by two elements:

- Smart Remote Services gateway software (residing on the computer) initiates and maintains a consistent connection to the SRS Enterprise servers through the virtual network adapter via the site connection to the Internet.
- Smart Remote Services Enterprise system

In both cases, the SRS Gateway component connects to the Smart Remote Services Enterprise system through an internet connection supporting HTTPS requests on port 443. SRS provides both ongoing remote monitoring of connected Siemens Healthineers devices and as-needed remote desktop support. However additional security measures in place are slightly different in our Atellica Connectivity Manager which is a software only product and in our *syngo* Laboratory Connectivity Manager.

c. Atellica Connectivity Manager (ACM)

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

An administrator account is built in for Siemens Healthineers service personnel. There are additional service user accounts that are required to effectively manage functions of the product. When issues arise, Siemens Healthineers service personnel may need to access the instrument desktop. Siemens Healthineers service personnel will log into the remote support enterprise system and request a live connection to the instrument.

Session control
Define the access available to remote users through the SRS Gateway GUI (instructions separately provided). You have full control over file uploads, downloads, and remote desktop access to your devices. Operators can grant or deny access to remote access sessions, software updates, and application access. If a computer issue arises, you can request a remote access session from Siemens Healthineers service personnel only.

The connection to the instrument is established over a virtual network adapter via the site connection to the Internet. Once the connection is made, you receive a pop-up message that you must acknowledge or the session will terminate.

When using SRS with a VNC session, the User Account Control (UAC) prompt can cause the VNC session to disconnect. Siemens Healthineers recommends enabling VNC auto-accept prior to accepting an SRS remote control session to reduce the number of connections you must accept. Auto-accept can be disabled when the remote control connections are no longer needed.

In the case of connected instruments that support remote desktop access through Smart Remote Services with TeamViewer, you must provide the Siemens Healthineers service personnel with the TeamViewer passcode. (The TeamViewer application is provided by the connected instruments.)

d. *syngo* Laboratory Connectivity Manager (LCM)

Access control
SRS personnel use a personal username and password for logging on and authentication to the SRS Enterprise system. All interactions between Siemens Healthineers service personnel and the hospital or laboratory's connected instruments are through the SRS application. All Siemens Healthineers user and system interactions are recorded and available for audit.

Session control
The customer can define the access available to remote users through the SRS Gateway GUI. Instructions are provided in a separate customer-facing document. The customer can have the benefit of full control over file uploads, downloads, and remote desktop access to their devices. Operators can grant or deny access to remote access sessions, software updates, and application access. If a computer issue arises, customers can request a remote access session from Siemens Healthineers service personnel only. An administrator account is built in for Siemens Healthineers. There are additional service user accounts that are required to effectively manage functions of the product that shall not be removed or modified.

SRS Remote desktop sessions are initiated on an as needed basis, and are usually related to investigating equipment issues. Remote desktop support is provided through SRS using an implementation of VNC (Virtual Network Computing) on port 443. Siemens Healthineers service personnel logged into the Smart Remote Services application can request remote access to an instrument connected to the private network. The request must be accepted by the customer 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 SRS server logs the remote connections and file transfers. In all cases, the local user must accept the remote desktop session to allow the remote user to continue. Remote Desktop support to connected devices through TeamViewer is facilitated by *syngo* LCM. TeamViewer is not used to access *syngo* LCM itself. However, some Siemens Healthineers devices may use TeamViewer in place of VNC.

Network control
SRS supports the following:

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

Data transfer
All data is encrypted during data transfer from the computer or connected instruments by Smart Remote Services personnel.

Remote monitoring can be initiated by the *syngo* LCM computer to the Smart Remote Services Enterprise system. The *syngo* LCM computer facilitates the transfer of test results, system errors, monitored properties, and files initiated by devices connected to the private instrument network. Requests for file transfers or support data made by Siemens Healthineers service personnel logged into the SRS application are forwarded to instruments on the private network through the *syngo* LCM computer.

3. Security measures for information in transit

To securely transport your data between your environment we offer different mechanisms to encrypt the connection. If you additionally opt to route all network traffic through your own firewall you will obtain full control over your communication.

a. Virtual Private Network (VPN) over the Internet
We use a state of-the-art IPSec solution to connect both environments. For mobile systems, we also offer a Transport Layer Security (TLS)-based VPN between your system and our DMZ.

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

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

Our VPN endpoint is also a Cisco router. In the event of incompatibilities to set the connection, please contact your local Siemens Healthineers representative.

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 DMZ to the system (see section 4). They also prevent access by Siemens Healthineers to other parts of your network, and access by third parties.

- **IPSec**

To prevent network sniffing and data tampering Siemens Healthineers uses the established standard IP Security (IPSec) 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. IPSec enhances data privacy using high level encryption with algorithms AES, or AES-GCM (AES-128, AES-192, AES-256, AES-GCM 128, AES-GCM 192, AES-GCM 256) and protects data integrity by up-to-date hashing algorithms method SHA-256, SHA-384, or SHA-512. Various Diffie Hellman Groups (14-2048-bit, 15-3072 bit, 16-4096 bit, 19-256 bit ec , 20-384 bit ec, 21-521 bit ec, 24-2048/256 bit) can be used for key-exchange security.

- **Optional debugging capabilities**

If you want to receive service router SNMP or Syslog messages on your router, or to see the current service router configuration, contact your local Siemens Healthineers representative.

b. Security measures for Internet-based connectivity
Internet-based connectivity (IBC) is based on the SRS security concept which uses TLS technology . This technology provides a secure and private communication channel for data exchange between the system and the SRS environment by establishing a direct encrypted network tunnel. This supports data protection and prevents virus infection from unauthorized third parties during an SRS connection.

VPNs utilizing TLS are quickly being recognized throughout the industry as a highly viable and economical solution for remote access. IBC allows customer systems to be connected to the SRS portal based on an Internet connection with no additional hardware or network requirements, thus offering greater system mobility without significant compromise on SRS connectivity and data security.

c. Transmission from your systems to the remote server
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 lifecycle and can therefore not be generally quantified.

- **User initiated transfers**

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

Data "pulls" are necessary when our qualified Customer Care Center service personal first try to troubleshoot a reported issue by using the log data stored on the customer system locally. If this is not possible and further support from experts is required, the Remote Service Engineer can initiate a data transfer to the Siemens Healthineers' Headquarters. This data is accessible to the specialists at the Customer Care Center, Remote Service Center and the Headquarters Support Center, including the product R&D team. In specific error cases, it might be necessary to also 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 encountered issue. The service personnel are trained how to handle data potentially containing PHI/PII.

- **System initiated transfers**

Automatic data "push" transfers happen at pre-defined points of time and in regular intervals. The transfers are done via file transfer and in a limited number of systems through emails from the system to the SRS DMZ. The data transferred during Auto-Push Transfers is "Technical Data", consisting of: application logfiles, errors, device properties (Technical Status Information) and configuration settings, software versions, patches, available licenses, network settings, device service history (Asset and Configuration Data) and sequences or performance of various tasks, used applications and interactions with the application (Utilization Data), and correlated data supporting predicting potential malfunctions (Smart Technical Data). These data are in each case not related to an identified or identifiable natural person.

When performing SRS-based services, Siemens Healthineers uses "Technical Data" to access, maintain, repair, calibrate, update or patch your systems or provide Remote Training or carry out additional system monitoring services supported by the Product or for own business, research or development purposes (e.g. for the further development of our products and services). This intended use has to be agreed upon upfront in the respective SRS Terms and Conditions agreement.

4. Security measures in our SRS Infrastructure

Our Smart Remote Services rely on the secure operation of our SRS platform and the "demilitarized zone" (DMZ) between the Siemens Healthineers Intranet and the Internet. The following measures are in place to enable Data Protection in our SRS backbone.

a. Authentication and authorization
The central maintenance platform (SRS portal) used by the Customer Care Center is hosted in an isolated segment of the company intranet. Access is restricted via PKI and / or One Time Passwords as second factor authentication mechanisms.

The granularity of our authorization concept allows us to define which users can access which systems. In practice, this means that our Service Engineers/Application Experts can only directly access those customer systems for which they are explicitly authorized and can only perform the functions they are authorized to conduct.

In addition to the access by Siemens Healthineers employees, our Business Partners also require access to our Smart Remote Services. Our Business Partners are also required to use two factor authentication and logging requirements we have implemented for Siemens Healthineers employees.

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

c. Demilitarized zone
Between your network and the Siemens Healthineers' intranet we use a Demilitarized Zone (DMZ) that prevents direct connectivity between both environments. Mirroring of your communication with our DMZ server towards our Intranet is only authorized under certain protocols. This architecture is designed to mitigate the risk of unauthorized network access through a reverse proxy server, thus hindering the transmission of malware between our respective networks.

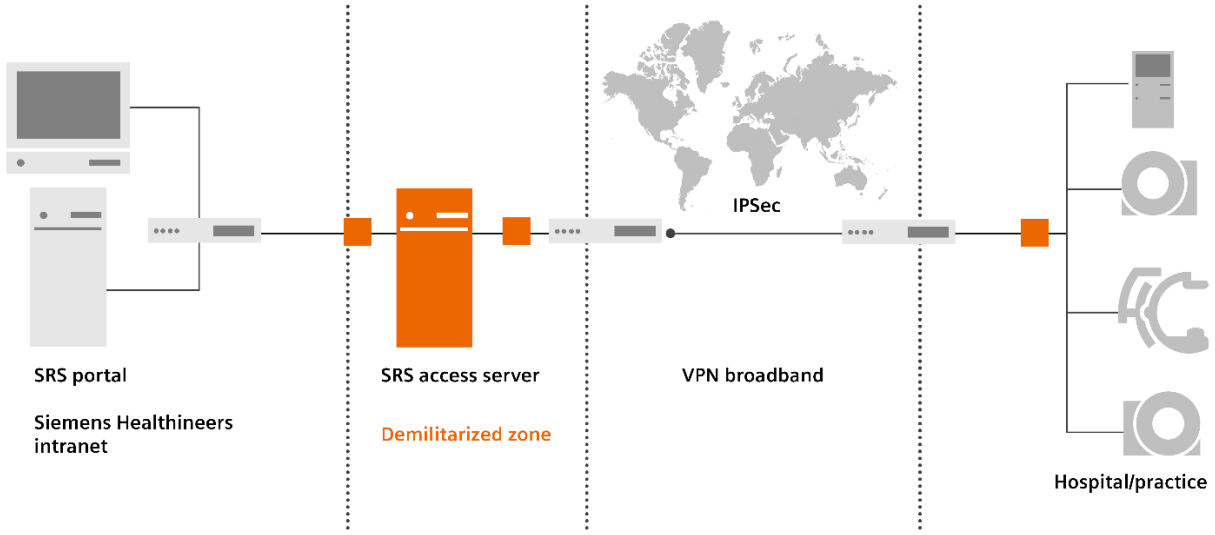


Figure 4: Security infrastructure of SRS

d. Protected SRS servers
The SRS access server is a Linux server operated according the Siemens Healthineers Information Security guidelines. The effectiveness of the protection measures is audited on a regular basis that the SRS servers are operated with state-of-the-art technology.

e. Organizational measures
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. This has been certified by TÜV Süd in Germany according to the international standard ISO 27001.

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 selected service employees and their corresponding access rights.

5. Protection against malicious attacks

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

a. Malware infections
By connecting your systems to SRS, your connection to our secure DMZ is also secured by state-of-the-art technology. As long as the Internet access is used for SRS purposes only, and the product is operated according to its security whitepaper, virus infections are unlikely.

b. Malicious e-mail traffic
Certain types of systems send e-mails to the SRS access server. These emails are sent in the direction from your system to our SRS environment. E-mails sent from your system to the SRS access server are forwarded to the appropriate Siemens Healthineers mail server and then relayed to the recipient which could be email addresses from Siemens Healthineers or from your own IT department. Each recipient address has to be whitelisted before email relaying is allowed. The Siemens Healthineers mail server scans all e-mails for viruses and reacts in accordance with the Siemens Healthineers security guidelines to observe that there is no threat to the Siemens Healthineers intranet. No e-mails are sent from the DMZ to the medical device.

c. Cross system infections
Cross infection between the Service Engineer workplace and the customer system is unlikely because there is no direct IP routing between them (refer to the reverse proxy function in section3).

6. How to further support your equipment?

Despite our firm commitment to cybersecurity, the nature of our different products may require your involvement to help you run them securely. All our equipment and software only products are released with a Security Whitepaper 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 equipment, and the additional considerations to set up the IT infrastructure around it to support a secure operation. Please refer to your Siemens Healthineers Customer Services representative for the Security Whitepaper of your Siemens Healthineers equipment.

7. FAQ

Does Smart Remote Services (SRS) allow Siemens Healthineers to access patient data on the connected system?

There are two scenarios in which we connect to the system through SRS:

In a remote diagnosis and repair scenario, Siemens Healthineers technical experts access only technical and maintenance data. If personal data or PHI is required to investigate the problem, the customer is informed in advance and must allow the access to the data. See section 1.a for further information.

The second scenario is a Remote Assist session. In this case, the user must actively grant access and acknowledge a disclaimer before the Siemens Healthineers employee is able to see the screen of the system which can contain sensitive information. See section 1.b for further information.

Can a service engineer connect to one of my systems without my permission?
Permanent access to the system can be enabled upon demand in the *syngo* applications software. This access can be revoked at anytime. Alternatively the software may be configured so that every remote service activity has to be expressly approved by you[4)]. Exceptions might apply.

Please see section 2.a for further information.

I don't want to approve every single remote service activity, but I want to be informed about them. How can you do this?
We can activate an e-mail service providing you the connection details before and after remote connection.

How does the user know that a remote service activity is in progress?
A visual indication on the bottom right corner of the screen is displayed while an SRS session is ongoing. The user can terminate any session at any time if desired. In this case, all service programs currently running are immediately shut down in a controlled manner. Please see section 2.d for further information.

How do you ensure that only authorized Siemens Healthineers personnel and business partners have access to the connected systems?
The access to the remote maintenance and support functions on your systems is restricted through two levels of control in our SRS infrastructure:

Two factor authentication: Employees or business partners require a two-factor authentication using either

a. SRS User ID, smartcard and PIN

b. SRS User ID, password and onetime PIN via SMS or email

Need to know principle: employees or business partners can only access systems for which they are expressly authorized.

Please see section 4.a for further information.

How is the connection between the SRS server and the hospital network protected?
The SRS server connects to the hospital network through an IPSec-secured VPN connection. For mobile systems that shall have a direct connection to the SRS server, we can provide an TLS-based VPN connection .

Please see section 3 for further information.

I am worried that the SRS connection creates vulnerability in the cybersecurity of my hospital's network. Wouldn't it be safer to not have the system connected at all?
To prevent Cybersecurity attacks on hospital (or any other) networks we recommend following the principle of security in depth and implementing strict security policies in all layers of the IT infrastructure. This means that all network devices, operating systems, application software office and clinical IT devices have their own adequate security controls to protect themselves from overseen flaws in the other IT elements.

The SRS security solution provides a state-of-the-art implementation to control and limit access to your network which hinder attacks coming from our DMZ into your environment. However, this is only an additional security layer to the protection measures you implement in your environment.

In addition, SRS is our fast channel to deliver 3rd party security patches when required. Therefore, unless otherwise stated, it is highly recommended to keep the connection to SRS in situations where new vulnerabilities affecting your equipment are disclosed.

Note: The content of this FAQ guide is based on the document CS SRS Security Concept Version 7.0 HOOD05162002929590. Refer to this document for more detailed information.

4) The described functionality is not available on server based systems like syngo.via server or syngo.plaza server.

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

If the service 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 pre-requisites that apply to certain service offerings).

Prerequisites: stable SRS connection with adequate bandwidth

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