How to get started

Important information/checklist for the IT administrator

Increasing the availability of medical systems is a key factor for boosting efficiency and profitability. With Siemens Remote Service (SRS), we provide a reliable IT infrastructure to do just that – based on a powerful and secure VPN broadband connection. Why? Because this technology offers many advantages: a high level of security, greater speed and efficiency as well as access to all SRS-based services such as Siemens Virus Protection, Siemens Guardian Program™ or Siemens Utilization Management.

To get started with establishing a site-to-site VPN broadband connection to our Siemens Remote Service infrastructure, all you need to do is go through the checklist on the backside of this flyer and provide your Siemens representative with the required information listed.

To make this as easy as possible for you, we have divided the steps to be taken into three groups:

- **Decisions to be made**
  on the infrastructure (router and last-mile technology) that should be used to connect your system/s to Siemens Remote Service.

- **Information to be provided**
  on the network configuration of each piece of medical equipment, the router and the configuration of the site-to-site connection.

- **Other things to be done**
  like opening the ports for communication.

Siemens Remote Service

Capitalize on a new dimension in system support.

SIEMENS

medical

Important information/checklist for the IT administrator

Decisions to be made

General

What type of endpoint do you wish to provide?	○ Your own infrastructure	○ Infrastructure provided by Siemens
Which kind of last-mile technology do you prefer?	○ VPN broadband/xDSL	○ I would like to use other solutions*

*Other solutions like e.g. ISDN are possible on demand. Please discuss this with your Siemens representative.

Regarding the IPSec configuration (our recommendations are marked in blue)

Session key setup

Authentication	○ **SHA 1**	○ MD 5	
Encryption	○ DES	○ **3DES**	
Key-exchange operation security	○ DH-768	○ **DH-1024**	○ DH-1536

Tunnel transformation

AH-authentication	○ SHA 1	○ MD 5	○ **none**
ESP-encryption	○ DES	○ **3DES**	
ESP-authentication	○ **SHA 1**	○ MD 5	○ none
PfS	○ **DH-768**	○ DH-1024	○ DH-1536	○ none

Information to be provided

On your medical equipment:

- IP address
- Gateway
- Netmask

About the endpoint:

- Name of manufacturer
- External IP address
- Internal IP address
- Netmask

Other things to be done

To enable your systems to perform all SRS-based services, the following ports need to be opened:

- Standard ports for communication**
- Ports for HP system management**
- Ports for CA system management**

** Please ask your Siemens representative for a list of ports.

For detailed information on the technical and organizational security measures we are taking to achieve a high level of security and privacy of patient data, please ask your Siemens representative for our SRS Security Concept.

www.siemens.com/medical