InSite™ Remote Support Concept

Unplanned medical system downtime can negatively impact every aspect of patient care - from patient productivity to staff productivity and cost control.

INDEX

INSITE™ - REMOTE SUPPORT CONCEPT

The three main components of the GE Healthcare Remote Support Concept

Proactive and Predictive Service

Hardware monitoring of the medical device

Reactive Application & Service Support by GE Healthcare Experts

Software Updates

Available via direct download on the medical device

> *Unplanned medical system downtime can negatively impact every aspect of patient care - from patient optimum care to staff productivity and cost control.*

InSite™ from GE Healthcare is a powerful remote technology that maximizes the uptime of your healthcare medical devices. Advanced digital tools constantly monitor your medical device system hardware and protect your Healthcare Environment from equipment failure and lost revenue.

With InSite™ Remote technology, GE Healthcare Support remotely troubleshoots performance issues and can forecasts maintenance of certain larger issues to reduce unplanned downtime - improving medical system efficiency and helping to reduce the cost of care.
InSite™ remote technology has been extensively integrated into the individual system components by GE Healthcare during the design of the medical device. Currently, there are +100K systems compatible with InSite™ globally.

For the proactive Hardware Monitoring, GE Healthcare uses Artificial Intelligence and proprietary algorithms for data-driven prediction and monitoring of your medical system components. Originally developed for CT imaging systems,

InSite™ technology has been adopted across GE Healthcare's networked medical devices to proactively monitor individual highly complex system components, notify GE Healthcare Service of fluctuations or deviations in the performance of individual components and, in consultation with the customer, forecast potential maintenance needs to minimize disruption of planned medical procedures.

34%

of cases are repaired remotely[1]

In a recent study done in a year more than 2500 CT systems across EU, USA, Canada and Japan, it's shown how the combination of GE's proactive and predictive solution (OnWatch & TubeWatch) is helping to reduce unplanned downtime by 41%[2], as well as Increasing the average planned labour hours up to 36% of the total onsite labour hours.[3]

CONNECT WITH CONFIDENCE

Constant monitoring. Continued support.

As soon as new medical devices from GE Healthcare are installed in your facility, throughout the agreed warranty period and for the duration of a service contract agreement, all InSite™ compatible medical devices will be connected to GE Healthcare's European InSite™ Remote Support environment. Through the GE Healthcare InSite™ technology, you can benefit from a comprehensive service offering, help you achieve exceptional value from each medical system, and deliver outstanding patient care.

To provide the best possible support for your clinical professionals, a medical device will need remote connectivity at day one of clinical operation.

All GE Healthcare commercial services and performance-optimizing offerings are built on an existing remote connection via GE Healthcare InSite™ Remote Support Standard.

If you have not yet signed a service agreement, our service staff will be happy to advise you on our flexible and comprehensive offers.

If GE Healthcare InSite™ Remote Support Standard was denied by the customer, GE Healthcare reserves the right to charge the customer for the additional cost of an on-site visit during the warranty period and in service contract coverage in accordance with the price list in effect at that time.

PROACTIVE AND PREDICTIVE SERVICES - HARDWARE MONITORING

Increased efficiencies.

Connectivity with InSite™ means GE Healthcare will proactively monitor your critical medical equipment, identify potential problems, and fix them before any workflow disruptions occur.

Proactive hardware monitoring is the core of the InSite™ technology. As more and more medical devices consist of highly complex mechanical and electrical components, the monitoring of many individual sensors and data measuring points is essential to keep the device in operation without any interruption in the demanding day-to-day medical environment.

The proactive monitoring services analyse and evaluate the technical functionality of the medical devices, it is designed to predict technical failures.
Monitoring relies on regular remote communication between the European GE Healthcare InSite™ Remote Network and the customer's medical device to retrieve specific technical data. Data processing takes place on the GE Healthcare's ISO 27001 certified European InSite™ Remote Support environment.

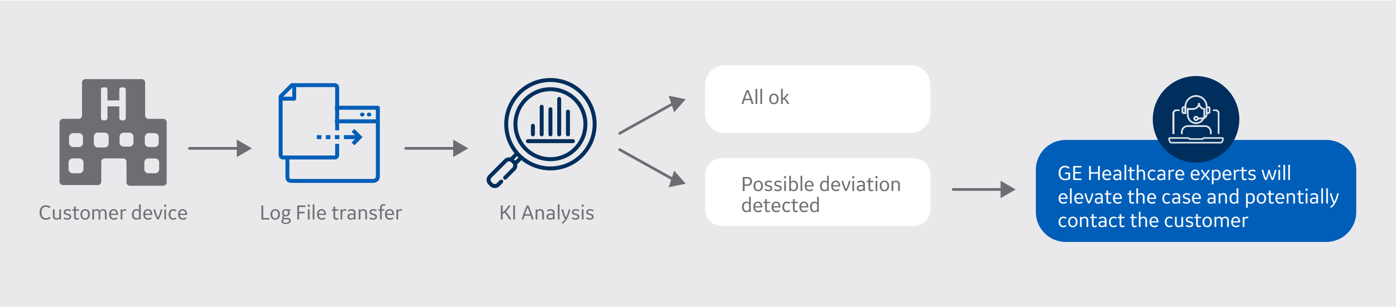
The technical data connection in details:
The customer's medical device is connected to the protected European InSite™ Remote Support Network via an encrypted data connection according to InSite™1 or InSite™ RSVP standard.

Automated server processes in the GE Healthcare InSite™ Remote Support network environment manage the hardware monitoring of all connected customer medical devices (Auto SC Server).

GE Healthcare Proactive Hardware Monitoring uses the latest technologies, such as Artificial Intelligence and proprietary algorithms for data-driven forecasting and monitoring.

The servers have a medical product-specific interval specification to download machine data from the connected customer medical devices. For this purpose, the server process contacts the customer medical device over the existing InSite™ remote connection and automatically downloads the technical log files (machine data). The log files are afterwards analysed fully automated by computerized server processes.
In the case of a deviation or a limit violation, a support ticket is automatically opened in the GE Healthcare service system for the affected customer medical device.

The support ticket will be assigned to the responsible GE Healthcare remote support expert to validate the deviation. The expert will initiate further steps to analyse and fix the customers' medical device problem in consultation with the customer.


Customer device
Log File transfer
KI Analysis
All ok
Possible deviation detected
GE Healthcare experts will elevate the case and potentially contact the customer

REACTIVE APPLICATION & SERVICE SUPPORT BY GE HEALTHCARE EXPERTS

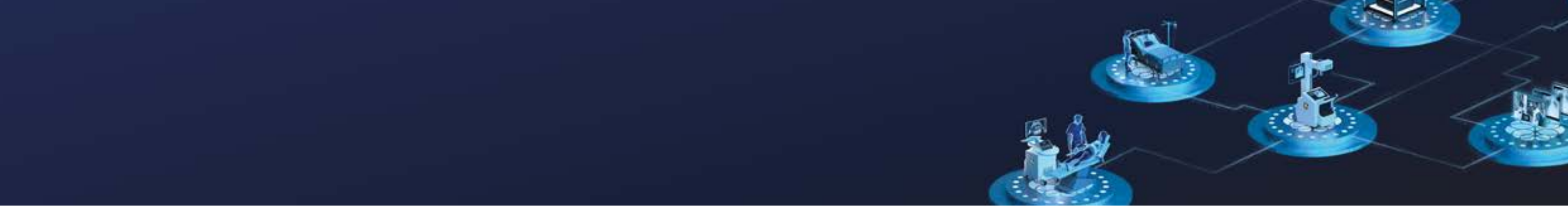
Continued support

> *All customer's medical device connected to GE Healthcare European Remote Support environment via InSite™ Remote Technology have direct access to our reactive application and service support by GE Healthcare experts.*

Only dedicated authorized GE Healthcare experts can connect into the GE Healthcare Remote Support environment from controlled GE computers via a secured portal solution. As a second barrier, a service support ticket from the GE Healthcare support system is always mandatory for the GE Healthcare experts to establish a remote connection to a customer's medical device in the portal.

A GE Healthcare Service Support ticket can be generated via the following interactions:

- the customer calls the GE Healthcare Service Centre,
- the customer creates a ticket directly on the medical device, using the iLinq or Contact GE function, or
- the customer creates a ticket directly in the MyGEHealthcare mobile application or via iCenter website.



The iLinq Service and Contact GE summons expert assistance with the click of one button on your medical device console. On-demand helps save valuable time by enabling your technologist to contact a GE Healthcare Experts from your medical device console. Your request will directly forward to our experts and there is no need to contact the call centre upfront.

Every interaction by GE Healthcare experts is documented in technical log files on the portal solution and in the related support ticket our experts summarize the performed activities for the customer documentation.

A GE Healthcare expert remote support session will standardly not have access to the customers' medical device screen with all patient data.

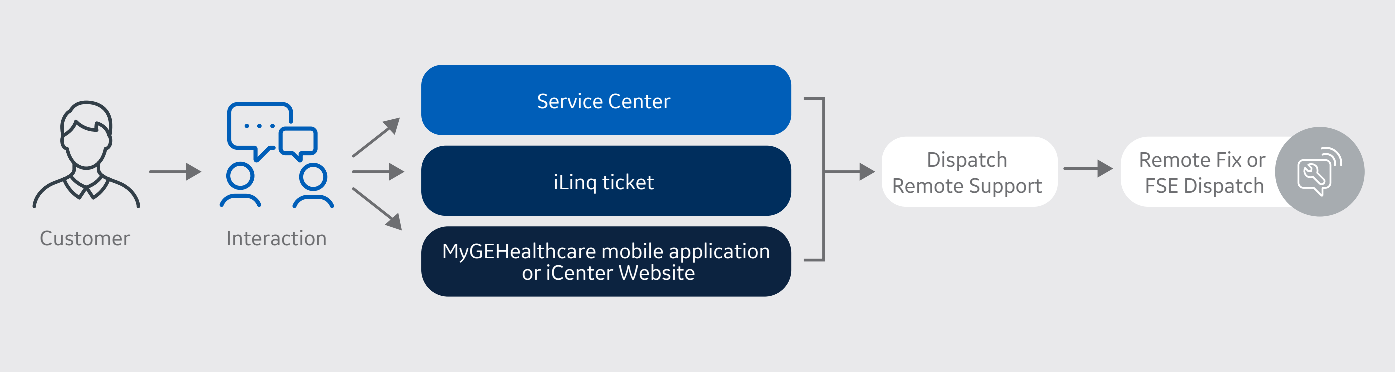
The experts connect into the backbone of the medical device based on technical protocols that are deeply integrated into the system.

A multi-level access model was integrated in the medical device, in the lower levels only technical data is accessible without viewing patient data. In the following levels, the patient data are pseudo-anonymized for the expert.

Only in the event that the medical user actively enables screen sharing on the medical device to troubleshoot a potential issue in the clinical interface, the GE Healthcare expert be temporarily able to view sensitive data.

The MyGEHealthcare App is the hassle-free way to manage your GE Healthcare service and support in one place—anytime, anywhere. Search "MyGEHealthcare" in the app store or Google Play, and download the MyGEHealthcare app.

https://www.gehealthcare.co.uk/services/my-gehealthcare-app

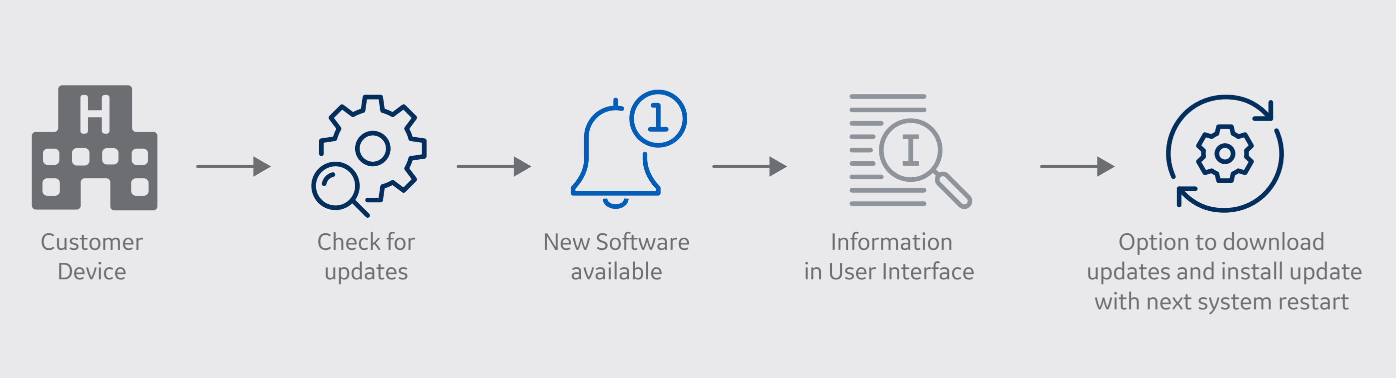

Customer
Interaction
Service Center
iLinq ticket
MyGEHealthcare mobile application or iCenter Website
Dispatch Remote Support
Remote Fix or FSE Dispatch

STAY UP TO DATE - SOFTWARE UPDATES*

> *In the next generation of medical devices, GE Healthcare delivers software updates to the customer directly in the system's user interface using InSite™ remote technology.*

Automated software download deployment significantly reduces the time required to update GE Healthcare medical devices. Any planned system downtime to manually execute updates and clinical workflow disruptions are greatly reduced.

If the software download functionality is activated on your medical device, the system will automatically receive all available software updates via the InSite™ remote technology. The clinical user will be informed about qualified updates via the system status dashboard and can open an overview of all available updates. By selecting and confirming the desired updates, they are automatically installed the next time the system is restarted.



Customer Device → Check for updates → New Software available → Information in User Interface → Option to download updates and install update with next system restart

* *Functionality depending on availability by product.*
The automatic software update function requires a permanent connection to the GE Healthcare European Remote Support environment via InSite™ remote Technology. Additional costs for an on-site patch deployment requested by the customer during the warranty period and in the case of service contract coverage will be invoiced based on the service price list.

InSite™ RSvP

InSite™ RSvP (Remote Service Platform), is the latest generation of remote connectivity by GE Healthcare integrated in the medical devices. It leverages secure connectivity to offer remote service and ensuring optimal system performance. The early warning of potential issues also heads off costly, unscheduled downtime and provides high system availability.

There are two technical components:

InSite™ RSvP Agent - software integrated in a GE Healthcare medical device.
InSite™ RSvP Servers - secure Web Services servers residing within the European GE Healthcare data centres.

The InSite™ RSvP Agent:

- Establishes secure communications to the European InSite™ RSvP Servers via the Internet.
- Monitor device performance data on an ongoing basis.
- Sends fault information and log files to the European InSite™ RSvP Servers.

What is communicated?

When a device sends a communication (polls), it does the following:

- Identifies itself to the European InSite™ RSvP Servers
- Responds to the last command it received from the European InSite™ RSvP Servers.
- Receives any new commands that the European InSite™ RSvP Servers has for it.
- Provides any new data it has for the European InSite™ RSvP Servers (such as files or attributes).

How frequently do communications occur?

Medical devices do not communicate continuously with the European InSite™ RSvP Server. Configuring assets to poll at a known rate allows for steady communication. The frequency of communication between a device and the European InSite™ RSvP Servers is called the poll rate.

Knowing how often an asset is supposed to poll allows the European InSite™ RSvP Server to detect when the asset is offline and may have an issue. The poll rate is also needed to perform certain tasks, such as Log-file transfers or remote support.

Default poll rate versus fast poll rate:

- The default InSite™ RSvP Agent poll rate is two (2) minutes.
- When a remote session is opened, the poll rate changes to fifteen (15) seconds to expedite servicing.

Connectivity overview:

The InSite™ RSvP Agent establishes connectivity from behind the safety of the customer's firewall; adhering to all security policies set by customer network administrators. The only networking requirement is: Outbound Internet access for the medical device using Transport Layer Security (TLS) over TCP port 443 (an HTTPS connection).
The connectivity is always one way, going from the RSvP Agent on a medical device to the European InSite™ RSvP servers.

Security details:

The following specifications apply to connectivity between the InSite™ RSvP Agent on the medical system and the European InSite™ RSvP Server:

- Transport Layer Outbound TLS/HTTPS connections
- Encryption Technology FIPS 140-2 level 1 or better
- Cipher Suite TLS 1.2, AES 256 bit (varies by Agent version and server deployments)
- Certificate Key RSA 2048 bits
- Signature Algorithm SHA256 with RSA
- Encryption in transit and encryption at rest
- Zero open inbound ports are required for the RSvP Agent
- Supports IPv6

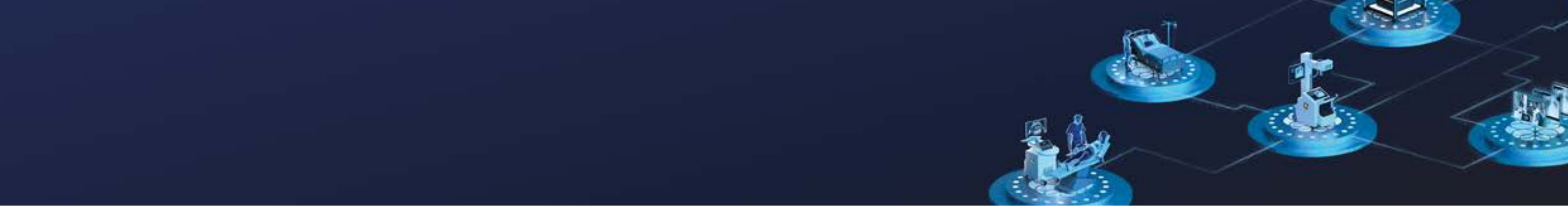
Validated End-to-end encryption:

A man-in-the-middle attack or any interruption (e.g. SSL-Inspection) between the validated InSite™ Agent and the European GE Healthcare InSite™ server endpoints will fully stop the InSite™ connectivity and any further data transfer will be denied by the European InSite™ RSvP Server.

Customer network requirements:

The GE Healthcare-serviced medical device must reach GE Healthcare European InSite™ Remote Support environment via the internet.

Customer security network environment (firewall) configuration must whitelist the European GE Healthcare InSite™ server URLs:
- https://insite-eu.gehealthcare.com:443
- as1-insite-eu.gehealthcare.com:443
- https://download.flexnetoperations.com:443
- https://gehealthcare-ns.flexnetoperations.com:443

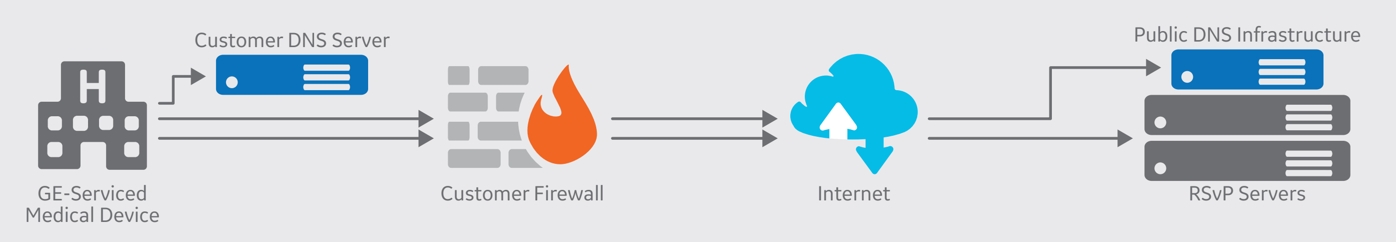


Customer network Connection Options:

Network connection options are based on the customer's site-specific needs.

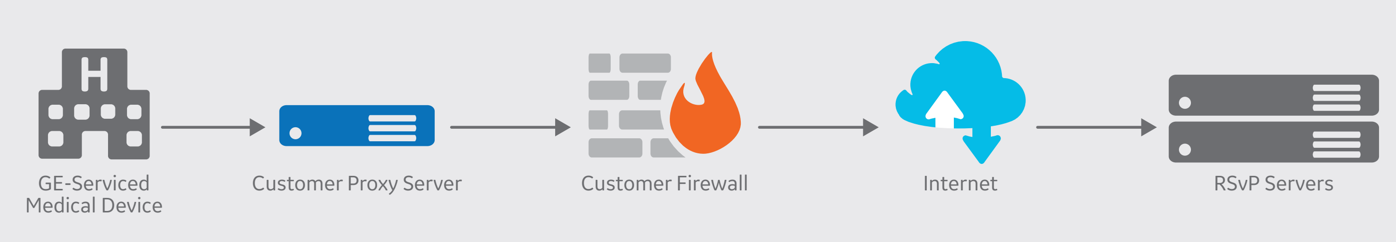
Direct Internet via public DNS resolution:

The GE Healthcare-serviced medical device connects to GE Healthcare Remote Servers via direct internet access and uses internal customer or external public DNS server IP addresses that must be configured on the GE-serviced medical device.



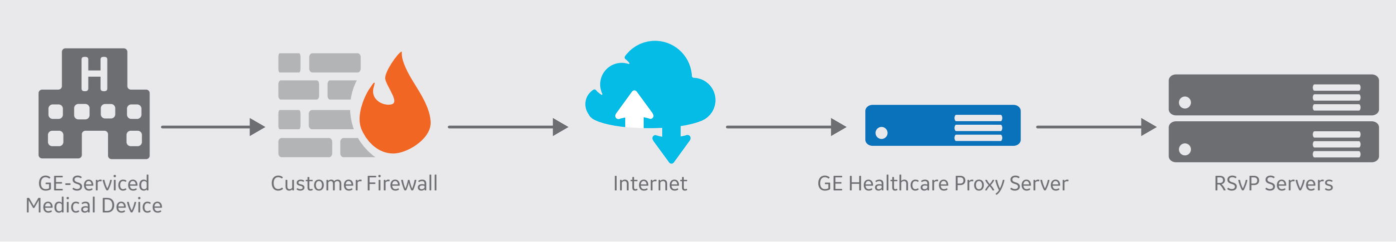
Internet access via customer-provided proxy server:

The GE Healthcare-serviced medical device connects to GE Healthcare Remote Servers via a customer-provided proxy server. The proxy server IP and port must be configured on the GE-serviced medical device. This may also be accomplished by configuring the DNS and a proxy server domain name.



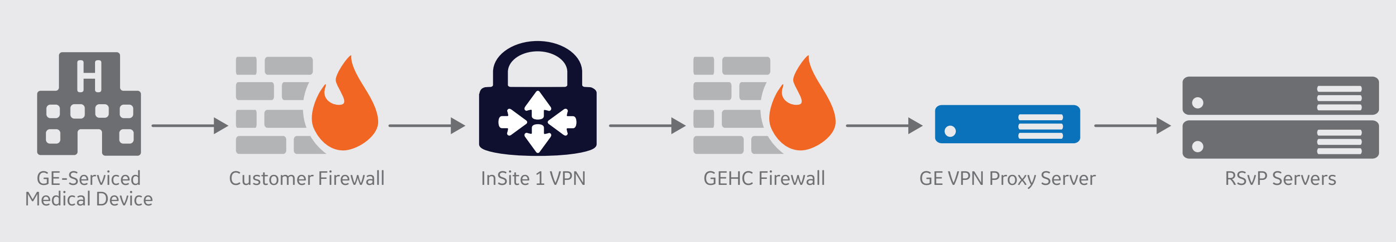
Internet access via GE Healthcare secured proxy server:

The GE Healthcare-serviced medical device connects to GE Healthcare Remote Servers via a GE Healthcare-secured proxy server. The GE Healthcare proxy server IP and port must be configured on the GE-serviced medical device.



GE Healthcare VPN connection (Site-to-Site IPSec VPN):

The GE Healthcare-serviced medical device connects from the customer medical network to GE Healthcare Remote Support network via an IPSec 24/7 VPN remote connection to the GE Healthcare Remote Servers. The GE Healthcare VPN proxy server IP and port must be configured on the GE-serviced medical device.



InSite™ 1 (SSH, SFTP, VNC, RDP)

The InSite™ 1 remote technology is the first-generation of GE Healthcare remote support technology. It was primarily focused on providing reactive remote services to customers and was upgraded with Proactive hardware monitoring.

How is the connection established?

Between the customer's Internet firewall / router endpoint and the European GE Healthcare Remote support environment endpoint a 24/7 IPsec Virtual Private Network (VPN) connection will be established.

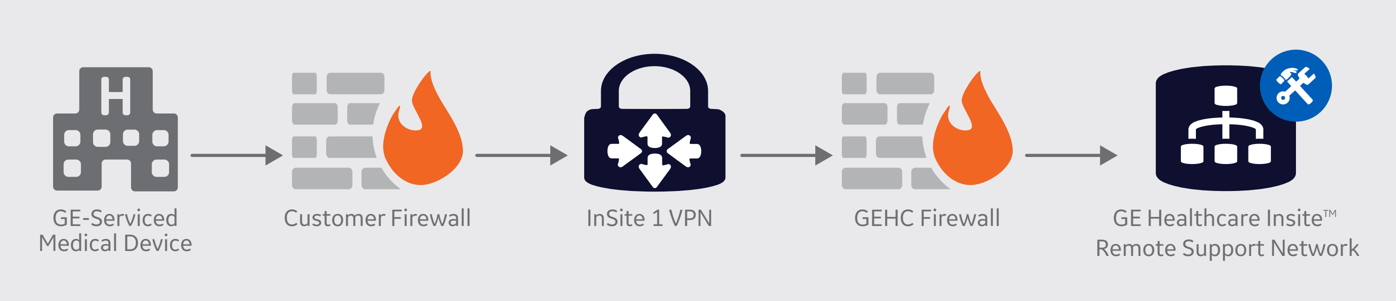
Via the VPN, all customer data traffic is routed through an encrypted virtual tunnel. VPN is a combination of tunnelling, encryption, authentication, and access control technologies and services used to carry traffic over an IP-based network.

Requirements for the customer medical device:

- The medical device requires a static IP address in the customer network.
- The medical device must have a routable network connection to the customer's Internet firewall / router endpoint.

Requirements for customer VPN hardware:

- Secure and permanent Internet connection with a minimum of 5 Mbps available.
- VPN compatible device (router, firewall) supporting the minimum GE Healthcare VPN connection and security parameters.
- Customer medical devices routable to GE Healthcare Remote Support environment address space (150.2.0.0/16) through the customer local network environment and the customer VPN device.
- GE Healthcare Remote Support tools utilizing a suite of network protocols and ports, each must be permitted to flow on/from your local network to the GE Healthcare European Remote Support environment.
- VPN type is mandatorily IPsec 24/7 site-to-site VPN with pre-shared key or Authentication Certificates.


GE-Serviced Medical Device
Customer Firewall
InSite 1 VPN
GEHC Firewall
GE Healthcare Insite™ Remote Support Network

GE Healthcare Remote Support environment address space (150.2.0.0/16):

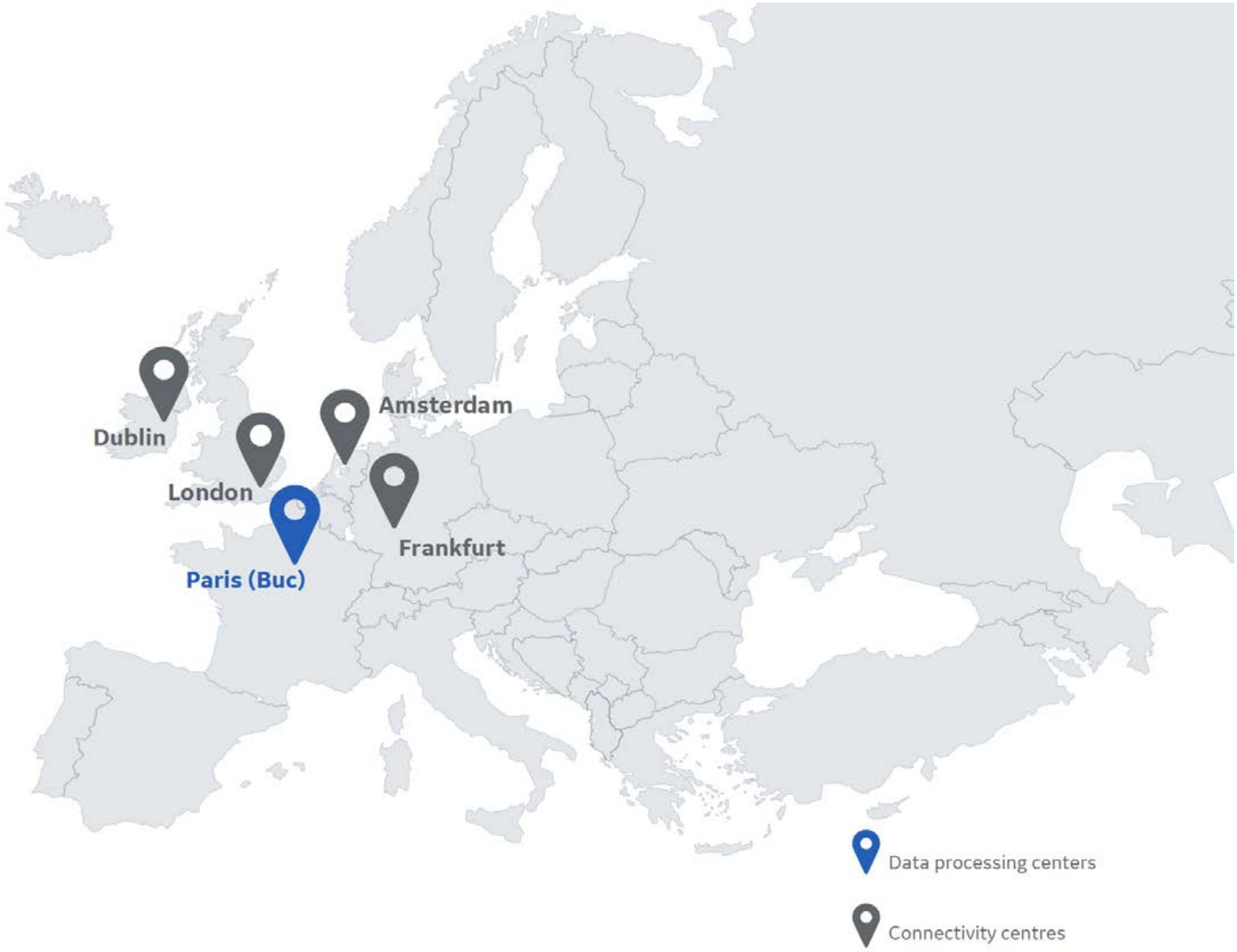
Since the first remote support network was built, the GE Healthcare InSite™ remote support network has been built on GE Healthcare's own address space: 150.2.0.0/16. Over the decades, the GE Healthcare Remote technology has continually evolved, and the technology has been deeply integrated into new products.

- The 150.2.0.0/16 is owned by GE Healthcare International, through GE Healthcare Japan Corporation. The proof of ownership can be reviewed via the Japan Network Information Centre (JPNIC): http://whois.nic.ad.jp/cgi-bin/whois_gw
- The 150.2.0.0/16 address space is not Internet-routable and is used only for the GE Healthcare InSite™ remote support environment.
- Even though a Class-B network can theoretically contain up to 65536 hosts, the number of servers in the GE Healthcare European Remote Support environment entitled to connect to customer medical devices are less than 100.

The InSite™ remote technology from GE Healthcare do not support any customer owned client-VPN solutions or any customer website portal solutions. Our GE Healthcare Experts are not allowed by policies to install a customer owned client-VPN solution or any customer website portal solutions software on a GE controlled computer.

Server locations

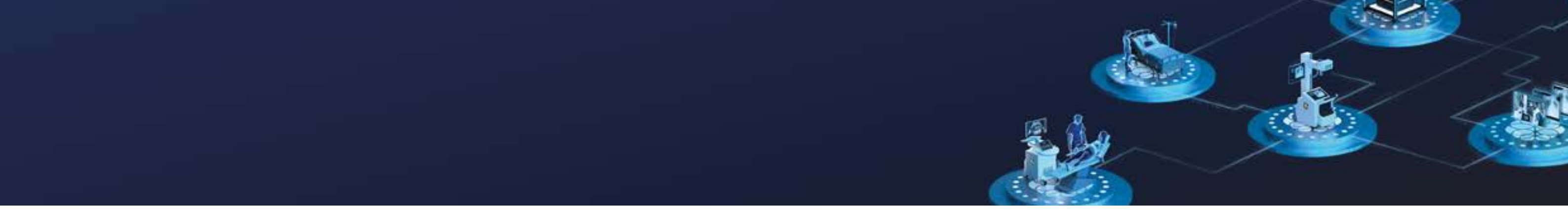
GE Healthcare main data centre for storage and processing is located in at our GE Healthcare facility in Buc, France. Additional connectivity data centres are located in Dublin, Frankfurt, Amsterdam and London (HSCN)



As a general practice, data from Europe is stored and processed in Europe.

All the resources that assist with local, national or European support in the field or remotely are located within Europe. Only in the case of L4 support (which typically requires of the assistance of Engineering teams), the expertise centres are located in numerous countries within Europe, but also outside Europe such as USA, Japan, India or China, depending on the location of the Engineering main hubs.

We ensure our internal and external suppliers involved in relevant processing, contractually meet our requirements and data protection obligations.

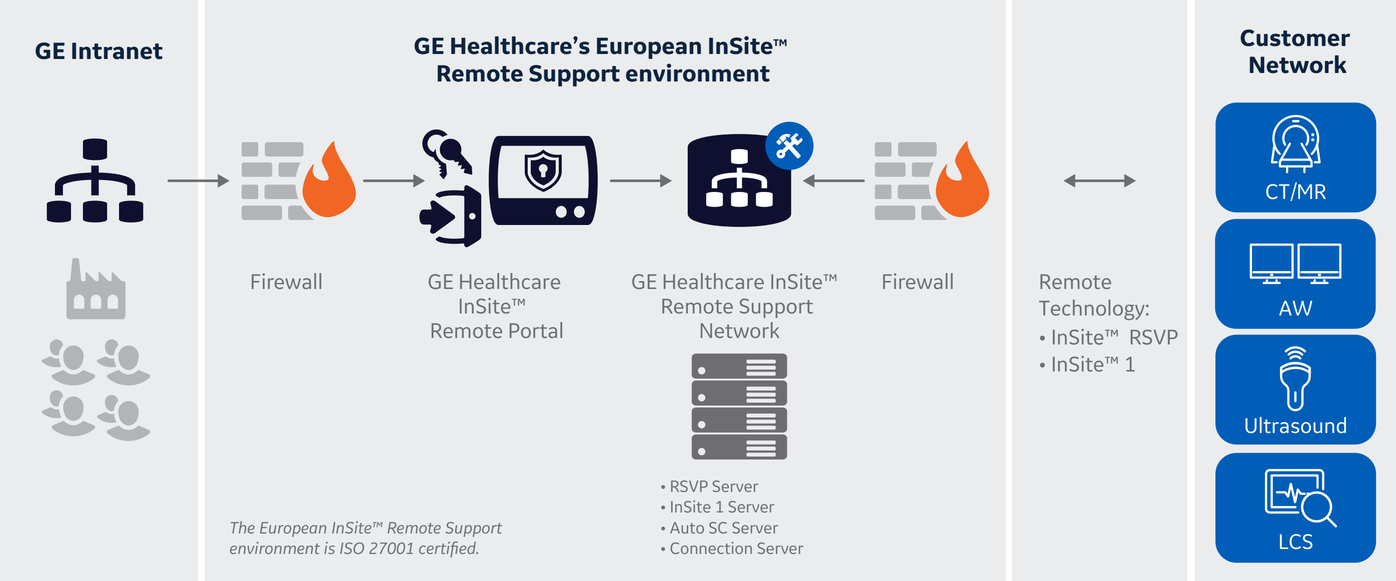


InSite™ Remote Support environment:

The European InSite™ Remote Support environment is a fully separated and highly secured network beside the GE Intranet.

Our GE Healthcare Experts have no direct access to the Remote Support environment or to any customer medical device.
Every remote connection from a GE Healthcare Expert to a customer medical device must be executed via a dedicated portal solution.

The portal solution has several technical security barriers to ensure the highest possible protection for our customers and their data:
- GE Healthcare experts must be trained and authorized on the medical device.
- Access require a multi-factor authentication (MFA) in the Remote Portal.
- The portal solution can only be accessed from GE computers in the GE Intranet.



The European InSite™ Remote Support environment is ISO 27001 certified.

Automated Support Central Servers:

Automated Support Central servers (AutoSC) are located in our GE Healthcare's European InSite™ Remote Support environment. The AutoSC servers are designed to securely automated GE Healthcare product engineering approved service tasks, like the proactive service for hardware monitoring of all connected customer medical devices.

AutoSC performs the following main functions:

- **Prodiags** - From the connected customer medical devices technical log files (machine data) are downloaded in a product-specific interval (up to every 2h). The log files are afterwards analysed fully automated by computerized processes with latest technologies, such as Artificial Intelligence and proprietary algorithms.
- **Sweeps** - GE Healthcare Experts request to gather specific technical data (machine data) from the customer medical devices on need-to-know basis to support an open customer service request. All sweep requests are pre-configured and validated by GE Healthcare medical product engineering. The sweep data are temporally stored on the AutoSC servers and are only accessible after login by the requesting expert.

ISMS - ISO 27001

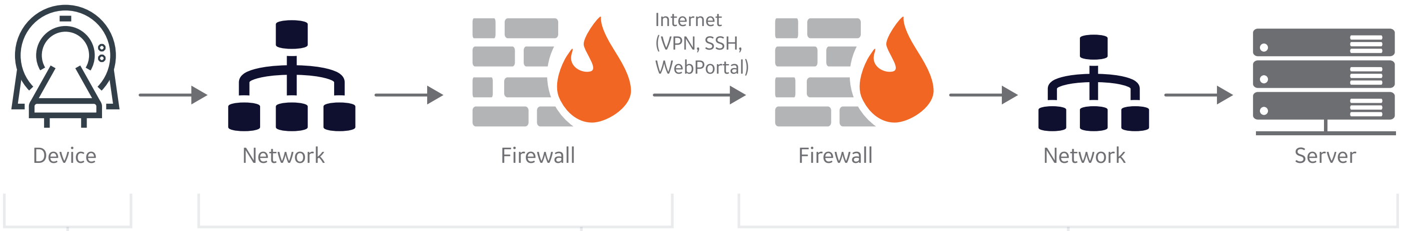
> *Since 2014, the European GE Healthcare InSite™ remote support environment has been independently assessed and certified wing-to-wing to ISO27001, the international standard and industry best practice. This certification underlines the robustness of our information security management. It also demonstrates that we assessed risks related to information security and established preventive measures to protect from information security breaches.*

Customer audited data protection framework

To improve customer and business partner confidence and ensure we are aligned with their requirements, our data protection framework is regularly reviewed by our customers.

bsi
ISO/IEC
27001
Information Security
Management
CERTIFIED

Comprehensive cybersecurity management framework



Product security

GE Healthcare follows a rigorous product development process to effectively address security risks. This includes risk assessment, inclusion of security controls in design requirements, continuous monitoring of new threats, documentation of controls and security features in user manuals and MDS2.

Hospital IT

Securing the hospital's physical and technical environment is critical to mitigate privacy and security risks when operating medical equipment and services.

Security Framework

GE Healthcare has implemented appropriate technical and organizational measures to protect your patient data and comply with data protection laws and regulations. We strive to continuously improve our processes, tools and controls to meet these obligations.

PRIVACY PRACTICES AND COMPLIANCE WITH PRIVACY LAWS AND REGULATIONS

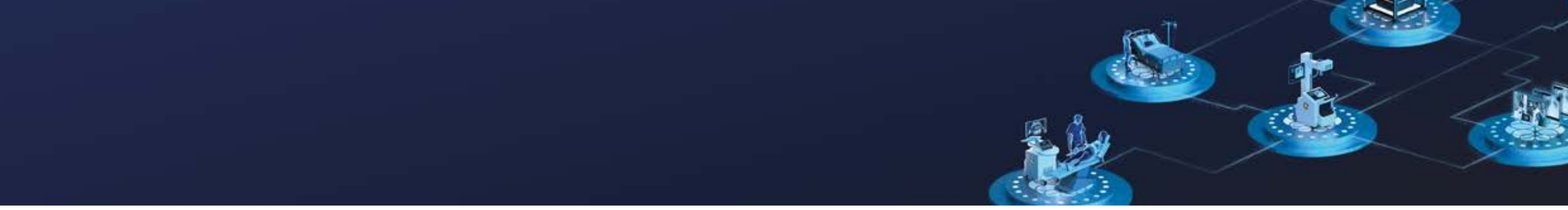
> *GE Healthcare takes the security and privacy of our InSite™ Remote Support environment very seriously. Maintaining the security of the environment is a top priority.*

GE Healthcare takes reasonable measures to protect the confidentiality, integrity, and availability of any Personal Data in its possession or control. These safeguards are comprised of a multi-tiered approach, including personnel security screening, workforce privacy and security training, physical access controls, network security, as well as techniques deployed on our medical products and the Remote Support environment themselves, such as password protection, firewalls, and where applicable, encryption techniques, logical access controls, and vulnerability management.

GE Healthcare continuously monitors its Remote Support environment and procedures to reduce risk against threats in the environment.

GE Healthcare respects the sensitivity of Personal Data and understands the importance of keeping this information confidential and secure. Since our goal is to provide the highest level of service to our customers and business partners, we want to share with you the comprehensive efforts GE Healthcare makes to comply with the applicable privacy and security laws and regulations.

Our policies, procedures and work instructions address the proper access to, use and disclosure of Personal Data by our workforce members and third party vendors, third party vendor qualification process and related vendor oversight, appropriate privacy and security contractual provisions (both with customers and vendors) and training of workforce members on privacy and security responsibilities. In addition, GE Healthcare's internal code of conduct- "The Spirit & the Letter" requires that, after more than 125 years, we still conduct our affairs with unyielding integrity.



European General Data Protection Regulation:

Compliance with European Privacy law (GDPR) requires a partnership between the customer and GE Healthcare when InSite™ Remote Services are in use.

You are taking care of your patients and their data.

We share this sense of responsibility.

GE Healthcare has developed an efficient GDPR framework to facilitate its implementation for the GE Healthcare InSite™ Remote Support Standard and all further commercial services and performance-optimizing offerings.

Each time GE Healthcare provides you Services, patient data is potentially processed, we need to ensure this is done in a controlled manner to comply with the rights of data subjects when handling their personal information.

The General Electric Company (GE) has implemented Binding Corporate Rules (BCR for Processing) in accordance with Article 47 of the GDPR.

The BCR are published on our website: http://ge.com/bcr gehealthcare.com

[1] Source: GE internal data for imaging (~32%) and ultrasound (~36%) systems coming from 2020.

[2] Versus a break and fix model.

[3] Average planned labor hours is calculated by using all the proactive service requests initiated by the system with their associated planned downtime compared to the number of service requests initiated by the customer and their associated unplanned downtime. Comparison is made by calculating the average across the three populations.

[4] Predictive solution = TubeWatch available for specific GEHC's CT products.