GE Healthcare's Commitment to Data Privacy & Security

Introduction

Today's healthcare environment is seeing rapid changes in the areas of data privacy and security, from recent updates to privacy laws to an increased risk of cyber-attacks, malware and security vulnerabilities. These events underscore the ever-changing landscape faced by health care providers and their business partners, such as GE Healthcare, in protecting the privacy and security of Personal Data they create, use, disclose and maintain. GE Healthcare is committed to safeguarding Personal Data in conformance with applicable laws, regulations, and industry practices.

GE Healthcare takes the security and privacy of its systems very seriously. Maintaining the security of our systems and the data they hold is, and always will be, 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 products themselves, such as password protection, firewalls, and where applicable, encryption techniques, logical access controls, and vulnerability management. GE Healthcare continuously monitors its systems and procedures to reduce risk against threats in the environment.

To that end, we are continually assessing the privacy and security capabilities of our products and services. We are committed to working with you to meet this evolving challenge.

Privacy Practices and Compliance with Privacy Laws and Regulations

Overview

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 code of conduct- "The Spirit & the Letter" requires that, after more than 125 years, we still conduct our affairs with unyielding integrity: http://www.gesustainability.com/how-ge-works/integrity-compliance/the-spirit-the-letter/.

How GE Healthcare Accesses Personal Data

In some cases, GE Healthcare may encounter Personal Data as part of the customer support and troubleshooting process or under other data access rights granted to us. We make best efforts to limit any access, collection, use, disclosure, and storage of Personal Data to only GE Healthcare authorised personnel and qualified third party vendors (as necessary and authorised) with a legitimate business purpose to provide support/troubleshooting services to our customers. These individuals are trained on the importance of properly safeguarding this information and they must comply with GE Healthcare's policies, procedures and work instructions, as well as applicable laws and regulations. We employ strict physical, electronic and procedural security standards to protect Personal Data and maintain internal procedures to promote the integrity and accuracy of that information.

Acceptable Use of Personal Data

GE Healthcare accesses, uses, discloses, and stores Personal Data only for legitimate, permissible business purposes and has implemented security safeguards and controls to protect this information. Personal Data is allowed only on GE Healthcare-approved systems or applications and handled only by authorised users. Any unauthorised access, use, disclosure, or storage of Personal Data is a violation of GE Healthcare policy, procedures, and work instructions. Any concerns over unauthorised access, use, disclosure, or storage of Personal Data must be reported and are investigated.

Third Party Vendor Access

GE Healthcare restricts third party vendor access to only those resources necessary to provide support/ troubleshooting services to our customers. Our vendors undergo a thorough qualification and vetting process managed by a global team of subject matter experts, including IT security and privacy professionals. Vendors connect to the GE Healthcare network through an isolated gateway segment that is monitored 24x7x365 for suspicious activity. Each vendor is assigned a business sponsor and interconnections are routinely audited to validate network access. Furthermore, any third party vendor that will create, receive, maintain, or transmit Personal Data on behalf of GE Healthcare and its customers is required to protect it in accordance with appropriate data privacy and security standards.

Remote Service Solutions

Overview
GE Healthcare has one of the world's most advanced portfolios of intelligent service and asset management tools for healthcare providers, all designed to improve the performance of our customers' systems. GE Healthcare's remote service solutions have been designed with significant security and privacy protections.

GE Healthcare employs two primary technologies for remote service. While these technologies differ, both were structured with a strong focus around security and privacy to protect Personal Data. Below are high-level overviews of each technology. For additional information around these technologies please contact your local GE Healthcare representative.

InSite 1 Technology
Our InSite 1 connectivity solution utilizes site-to-site Virtual Private Networks (VPN) to transfer service information bi-directionally between the customer and GE Healthcare. This solution combines tunneling, encryption, authentication, and access control technologies to maintain security during data transfer. The InSite 1 solution leverages your existing network infrastructure, internet connection, and firewall/VPN router to access your GE Healthcare equipment. This solution provides our customers with the ability to control and monitor GE Healthcare access to their imaging systems.

All data transmitted via InSite 1 is encrypted during transfer so that only authorized parties are able to access it. Minimum encryption level is 128-bit, but we recommend 3DES (168-bit) or AES (192-bit or higher).

InSite Express Connect (InSiteExC or InSite 2) Technology
GE Healthcare's InSiteExC is specifically designed to address the connectivity and security challenges posed by today's portable medical equipment. It enables remote diagnostics and repair, and application support with or without a fixed VPN connection. InSiteExC utilizes 128-bit or higher Secure Socket Layers (SSL) encryption, as well as password authentication and identity validation of devices, to maintain security during data transfer.

InSiteExC uses a three-layer security architecture based on Web services that achieves both transparency and security by employing security at the device, network, and enterprise layers. The end user or system initiates and ends all connections. This technology has been developed to prevent unauthorized changes or access to the system, as you are always in control.

Operationalising Data Privacy and Security in Remote Service
All GE Healthcare authorised support personnel must complete privacy training before receiving access to remote service tools. Only support personnel who have been granted access and have successfully completed multiple levels of authentication can access customer systems. Remote service activity is monitored and logged. Monitoring and logging contain, at a minimum, the following details:

- Purpose of the connection;
- Date/time of remote service activity;
- Protocol/technology used;
- Specific customer system connected to at the customer site; and
- Identity of the GE Healthcare individual or automated service system that established connectivity.

GE Healthcare remote service operations are provided by GE Healthcare OnLine Centers (OLC) that provide a secure connection to our customer networks through a logically-separated environment, managed by a multi-tiered state-of-the-art gateway. An extensive set of monitoring tools is implemented to enable detection of hardware or software failure, risk of failure, or security compromise of the OLC system. GE Healthcare security personnel closely monitor all servers, routers, firewalls, and intrusion detection/prevention systems 24x7x365. OLC computer and networking equipment are securely locked in an access-controlled Data Center with the following safeguards in place to protect Personal Data:

- Enterprise Antivirus / Anti Malware software that is updated weekly;
- Enterprise security patching and updating of operating systems;
- Whole disk encryption for portable devices;
- Unique user logins;
- Software assurance testing for applications implemented into hosting environments; and
- Physical security of data centers and facilities including badged access to data centers.

Our remote service infrastructure is periodically assessed for risk by a risk assessment team that uses a framework that includes Cobit, ISO and SSAE16 criteria to measure security capabilities and identify/mitigate security risks.

Product Cyber Security and Privacy

Overview
GE Healthcare follows a total Secure Development Lifecycle approach in designing and deploying products. This includes defining the appropriate risk-based design inputs early in the development process via our Design Engineering Privacy and Security (DEPS) process, secure coding and architecture, and security assurance testing. Our goal is to identify and mitigate risks based on the product function and typical user environment.

Design Engineering Privacy and Security (DEPS)
GE Healthcare recognises customer expectations and patient rights regarding the privacy and security of Personal Data both within the healthcare provider environment and in the conduct of GE Healthcare business activities. DEPS is the system of processes and controls that helps ensure that GE Healthcare products and engineering business activities meet privacy and security requirements for healthcare providers and patients.

Patch Management
GE Healthcare monitors patch releases for third-party software components. If a patch is applicable to a GE Healthcare product software component, the relevant design engineering team(s) will evaluate the patch applicability to the product design and/or function, and if applicable, perform testing of the patch in accordance with product design change management practices to ensure that the patch does not have an adverse effect on the function of the device. Patch status information is made available to customers via a web portal, as it becomes available.

Antivirus/Malicious Software protection
GE Healthcare will recommend use of anti-virus/anti-malware products when appropriate for product risk within the expected operating environment. GE Healthcare follows a risk-based approach for integrating security controls and features into product designs, and if appropriate based on overall product risk. GE Healthcare Engineering will evaluate and recommend for use one or more anti-virus/anti-malware products. GE Healthcare will recommend use of such products only following confirmation that the anti-virus/anti-malware product will not adversely affect function of the device.

Incident Response
We interact with sensitive patient information every day, and recognize the need to maintain vigilance over this data to help protect its privacy and security. GE Healthcare proactively utilises a combination of network monitors, log aggregators, and analysis tools, which provide alerts for viruses, worms, Trojans, and other malware. In addition, we also proactively scan all systems connected to the network to look for both vulnerabilities and for traces or side effects of malware.

GE Healthcare has also developed a robust incident response process for personnel to report data privacy and security events and concerns. When an incident is identified either proactively, through incident reporting, or via customer input, the appropriate internal teams are notified and immediately begin an investigation. The teams will then respond to the incident, taking action to implement the appropriate solutions and proactively identifying opportunities to reduce risk moving forward. GE Healthcare will communicate relevant issues and findings to customers, as well as provide recommended solutions, as the need arises.

If you have a concern or issue to report, please contact your local GE Healthcare representative immediately.

Data Privacy and Security Best Practices

GE Healthcare has taken many steps to ensure our operations have the appropriate security and privacy protections. That being said, customers are ultimately responsible for their own site network security, systems, devices, and databases and should implement formal policies and guidelines to protect their systems and data.

Healthcare providers must take steps to limit physical access to trained clinical staff where appropriate. User authentication is needed to ensure only authorised users perform clinical configuration changes, such as the setting of alarm limits. Point-of-care devices generally do not require user authentication for normal patient monitoring and surveillance since immediate access is required for making critical decisions about patient care.

GE Healthcare | 9900 W Innovation Drive | Wauwatosa, WI 53226 | U.S.A. | gehealthcare.com
Europe, Middle East, Africa DOC1668119 Rev 1.0, February 2015