GE Healthcare's Commitment to Cybersecurity

The healthcare ecosystem has faced many new security challenges over the past years. New digital technologies, greater drive for mobility, and increased remote connectivity and dataflow have widened the threat landscape for healthcare's connected infrastructure, while malicious actors are increasingly targeting healthcare delivery organizations.*

The increased concern from healthcare delivery organizations is shared by regulators, industry groups, and GE Healthcare. As a global leading medical technology provider, we take our role in helping to secure the healthcare ecosystem seriously by fully integrating cybersecurity into every aspect of the business, from product development to maintenance and support. Our cybersecurity organization reaches into every relevant area of the organization with policy-governed, well-defined, measured programs that are implemented across the entire product lifecycle to create an appropriate, effective, and risk-based approach to cybersecurity.

Our place in health security

With a myriad of imaging equipment in hospitals worldwide, and an environment in which clinicians use our devices to perform a multitude of patient examinations each year, patient safety is our top priority. Knowing the important role we play, the quality of our products and the integrity of our teams is reflected in the earliest stages of design and development. Our medical devices and solutions require systemic security threat and risk-based design, build, deployment, and support activities throughout the entire lifecycle. For us to succeed in these endeavors, we must work hand-in-hand with healthcare providers, ensuring that the appropriate operational security practices around device implementation and use are in place, following their own threat and risk-based processes.

As a leading medical technology and digital solutions provider, GE Healthcare plays a crucial role in providing health systems with the security and reliability they need today. We have a robust team of security experts in place and follow a comprehensive product security approach.

Our product security program has received significant investment and growth over the last few years as GE Healthcare has made a concerted effort to further the maturity of our security programs and drive greater transparency into how we assess and mitigate potential cyber risks throughout the lifecycle of our products. In addition to our Secure Software Development Lifecycle (SSDLC) process and managing our post-market lifecycle, we have enhanced our vulnerability management program to identify and communicate potential threats earlier, and be more proactive with customers in how we respond to those threats. We launched an exceptional security portal to notify customers of potential critical vulnerabilities impacting our products within three days of discovery, and generally share proposed remediation within 30 days (e.g. patching, mitigating controls etc.).

* Healthcare Breach Report 2021 Hacking and IT Incidents on the Rise. https://www.bitglass.com/blog/hacking-and-it-incidents-on-the-rise

We continue to engage stakeholders across the ecosystem and work with government organizations, regulators, healthcare providers, and security industry groups and leaders on cyber readiness initiatives that support the safe and effective use of our medical devices and software solutions. Through our Coordinated Vulnerability Disclosure Program, we encourage and support security researchers to proactively engage with us on any potential vulnerabilities and related disclosures in a coordinated, transparent and responsible manner. Ultimately, we are all working toward the same goal – enabling providers to diagnose and treat patients in the most effective way possible while maintaining the security of their medical devices. This collective effort will improve practices overall and help ensure the security of the entire health ecosystem.

Our vision

We are committed to developing and maintaining security in our products and services to meet the expectations of our customers and regulators. We continue to innovate in the medical device security space, to deliver security support and updates throughout the life of our products. We believe that a medical device needs to have a defined cybersecurity lifecycle plan from the day it is first launched until the day it reaches its end of support. We design, develop, test, and maintain our products with this mindset, and we continue to invest in new technologies and product architectures to build on this vision. Through our shared security responsibilities, we will continue to work together with integrity and transparency.

We believe that a medical device needs to have a defined cybersecurity lifecycle plan from the day it is first launched until the day it reaches its end of support

Our approach

Secure product development

We follow a total Secure Development Lifecycle approach in designing and deploying our products. This includes defining the appropriate risk-based design inputs early in the development process. Our goal is to identify and appropriately mitigate risks based on the product function and user environment.

DEPS: Design Engineering Privacy and Security is our secure product design and development process. It follows a rigorous set of principles that guide us through all stages of product development, testing, and preparation for the market. The DEPS principles are as follows:

- **We determine in the design phase** what the product or solution architecture will be based on its intended function, how it will be used, and in what environment it will operate.
- **A full threat assessment** is performed based on the initial design and operating environment using industry standard threat models specifically tailored to the clinical environment in which our devices operate.
- **Based on the threat model and subsequent risk assessment,** a customized comprehensive set of security controls is created (aligning with applicable standards, including NIST 800-53), which are required to be implemented during the development process.
- **Throughout the development process,** control implementation is continuously monitored and controlled through Quality Management System checkpoints.
- **In the final development stages,** manual review, vulnerability scans, static and dynamic code analysis, and several phases of internal and external penetration testing are performed to ensure full implementation of controls to help secure our products throughout their lifecycle.
- **Any findings emerging from testing** need to be addressed. Assessment findings are reviewed by the cybersecurity team, and are either fully addressed prior to release, or in rare cases with lower associated risks any residual risk is formally risk-accepted and documented.
- **Prior to release to the market, formal documentation is created** to describe any deployment-related controls for the customer to implement. A standardized hand-off of residual risk is a formal part of this documentation.

Since launching the DEPS process in 2013, we have trained more than 3000 engineers across GE Healthcare and applied the tenets across all new product development. We continue to evolve and improve the program by adding new architecture, design, and development principles to both the process and the overall build of products and solutions to stay ahead of new threats and security developments.

Lifecycle and vulnerability management

After products enter the market, GE Healthcare has a rigorous process that involves monitoring threats and vulnerabilities that could potentially impact the security of our products. We also solicit inputs from healthcare providers, researchers, internal tests, vendors, and other sources such as the National Vulnerability Database and deep domain expertise of our cyber team to keep up with new threats.

Outputs from these various processes and sources become important inputs that we incorporate into our vulnerability management process. Upon determining that a vulnerability poses a potential risk to any GE Healthcare product, we review the device software bills of material (SBOMs) through a specialized database and assessment tooling to identify devices containing the affected software.

GE Healthcare has a formal process to assess the risk associated with any vulnerability. The criticality of a vulnerability is determined per product based on standard assessment criteria. If the outcome of this assessment indicates a potential critical risk, we strive to post the details and product information on our customer accessible portal within three days. If GE Healthcare determines that a vulnerability poses a critical risk, our goal is to provide information on required software patches or updates, along with any recommended compensating controls, within 30 days. In rare cases, testing requirements and/or technical issues, such as product performance impact, may result in a delay due to the need for additional testing. If a software vulnerability has the potential to result in a critical risk and cannot be patched, GE Healthcare will recommend compensating controls where applicable. In some cases, GE Healthcare may address a critical security risk through a quality recall process. In such cases all regulatory requirements are followed. Our primary goal in this process is to provide timely information and help reduce risk, regardless of full (public) availability of mitigations by any involved parties.

All information related to vulnerabilities and patches are available at GE Healthcare's Product Security portal. At this site, customers can subscribe to email updates regarding new critical vulnerabilities and access security documentation related to GE Healthcare products, including the latest available MDS2 forms.

Anti-virus/malicious software protection

GE Healthcare recommends the use of anti-virus/anti-malware products when appropriate for product risk within the expected operating environment. The company follows a risk-based approach for integrating security controls and features into its product designs, and if appropriate, based on overall product risk, GE Healthcare will evaluate and recommend for use one or more anti-virus/anti-malware products. Any recommendation for such anti-virus/anti-malware solution requires GE Healthcare validation that the anti-virus/anti-malware product will not adversely affect the function of our device. We continuously assess the ecosystem and collect feedback from customers on the most suitable approach to anti-malware and adjust our validation strategy accordingly.

Operating system vitality is key to mitigating cyberthreats which are constantly evolving

Remote service

All GE Healthcare-authorized support personnel must complete security and 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.

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 gateway. An extensive set of monitoring tools is implemented to help 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 24×7×365.

OLC computers and networking equipment are securely locked in an access-controlled Data Center with the following safeguards in place to safeguard Protected Health Information (PHI) and Personal Identifiable Information (PII):

- Enterprise anti-virus/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
- Physical security of data centers and facilities, including badged access to data centers

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

An extensive set of monitoring tools is implemented to help enable detection of hardware or software failure, risk of failure, or security compromise

Remote service solutions

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 existing network infrastructures, Internet connections, and firewall/VPN routers to access 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.

InSite Express Connect (InSiteExC or InSite 2)

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 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 the customer is always in control.

InSite RSVP

The two major technical components of InSite RSvP are the agent deployed on the GE Healthcare-serviced medical device and the secure servers at GE Healthcare. This technology utilizes TLS/HTTPS as the main communication channel. The GE Healthcare-serviced medical device contacts secure GE Healthcare servers using an asset initiated outbound connection. InSite RSvP does not require any open inbound ports or a VPN connection. This solution utilizes the following key security elements:

- Transport Layer Outbound TLS/HTTPS connections
- Encryption Standard FIPS 140-2 level 1
- Cipher Suite TLS 1.2, AES 256 bit (varies by Agent version and server deployment)
- Certificate Key RSA 2048 bits
- Signature Algorithm SHA256 with RSA
- Encryption in transit and encryption at rest

Closing statement

At GE Healthcare, we are committed to helping clinicians provide the best patient care possible and enabling precision health through intelligent devices, data analytics, applications, and services. Our Product Cyber Security program supports these goals through implementing secure design and lifecycle support practices to help protect our products from the growing risks of cyber threats. GE Healthcare works with customers, regulators, industry groups, and other stakeholders in the healthcare ecosystem to implement collaborative and innovative practices for medical device security.

Our team of security professionals, and many additional employees with significant security training and expertise, are committed to creating a secure healthcare ecosystem. We will be more than happy to answer any questions that may arise.

JB18530XX