GE HealthCare's commitment to cybersecurity

The healthcare sector has encountered numerous security challenges in recent years. The introduction of new digital technologies, a growing emphasis on mobility, and an increase in remote connectivity and data transfer have expanded the range of potential threats to the interconnected systems within healthcare. At the same time, individuals or groups with malicious intent are increasingly focusing their attacks on healthcare organizations that provide medical services.[†]

As a leading provider of medical technology worldwide, GE HealthCare is committed to helping providers prioritize patient safety and enhancing the security of the healthcare system. We do this by incorporating cybersecurity measures at key stages of our business operations, including product development, maintenance, and support. Our dedicated cybersecurity programs are carefully measured and applied throughout the entire lifecycle of our products, ensuring that our cybersecurity approach is suitable, effective, and focused on managing risks.

GE HealthCare

[†] The Biggest Healthcare Data Breaches of 2024
https://www.hipaajournal.com/biggest-healthcare-data-breaches-2024/

Our vision

We are committed to strengthening cybersecurity in our products and services to meet customer expectations and regulatory requirements. We innovate in medical device cybersecurity, providing support and updates throughout the product lifecycle. Our products are designed, developed, tested, and maintained with a defined cybersecurity plan from launch to end of support, and we continually invest in new technologies to enhance this vision. Through our shared cybersecurity responsibilities, we will continue to work together with integrity and transparency.

Our place in healthcare security

As a leading provider of medical technology and digital solutions, GE HealthCare helps provide the security and reliability that health systems need today. Helping providers to focus on patient safety is our top priority, reflected in the quality and integrity of our products from design to deployment and we work in partnership with our customers to implement proper operational security practices. We have significantly invested in our product security program, enhancing our vulnerability management and proactive threat response. Through our Coordinated Vulnerability Disclosure Program, we work with security researchers to address potential vulnerabilities responsibly. Our goal is to enable healthcare providers to diagnose and treat patients effectively while maintaining the security of their medical devices, helping to ensure the security of the entire health ecosystem.

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.

Design Engineering Privacy and Security (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 the product's 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.

> 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

- **In the final development stages**, manual review, vulnerability scans, static and dynamic code analysis, and several phases of internal and/or external 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 are 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 product's Privacy & Security Manual.

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 rigorously monitors threats and vulnerabilities that could impact product security. We gather inputs from various sources, including healthcare organizations, researchers, internal tests, vendors, and the National Vulnerability Database. These inputs are integrated into our vulnerability management process.

When a potential risk is identified, we review device software bills of material (SBOMs) to pinpoint affected devices. We assess the risk associated with vulnerabilities based on standard criteria and strive to post details on our customer portal promptly. If a vulnerability poses a critical risk, we aim to provide information on necessary patches or updates, along with recommended compensating controls. In rare cases, additional testing may delay these updates.

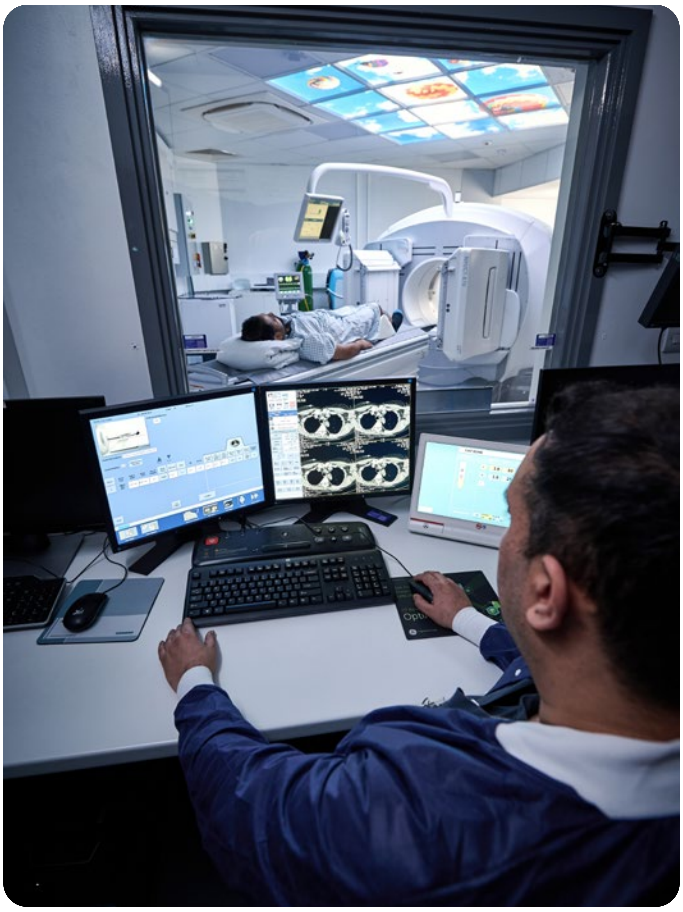
Operating system vitality is key to mitigating constantly evolving cyber threats

If a critical risk cannot be patched, compensating controls are recommended, and in some cases, a quality recall process may be initiated, following all regulatory requirements. Our primary goal is to provide timely information and reduce risk.

All information related to vulnerabilities and patches are available at GE HealthCare's Product Security portal (securityupdate.gehealthcare.com). 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 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 one or more anti-virus/anti-malware products. Any recommendation for such anti-virus/antimalware solution requires GE HealthCare validation that the anti-virus/anti-malware product will not adversely affect the function of our medical 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.



Remote service

GE HealthCare remote service operations are provided by GE HealthCare Online Centers (OLC) that utilize 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.

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

All GE HealthCare support personnel must complete regular security and privacy training in addition to product specific qualifications. Agents providing remote support must utilize an authenticated GE HealthCare issued device that is on the GE HealthCare network and be authorized, by their management, before they can gain access to our remote support tools. This approach allows us to provide security, accountability, and enables us to enforce non-repudiation for any remote connection our customers authorize.

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 requiring multi-factor authentication
- 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.

Cybersecurity is a critical part of patient safety

At GE HealthCare, we are committed to helping clinicians provide the best patient care possible and enabling precision healthcare through intelligent devices, data analytics, applications, and services. Our Product Cyber Security program supports these goals through the implementation of 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 helping create a secure healthcare ecosystem. We will be more than happy to answer any questions that may arise.

Visit **www.gehealthcare.com/support/home** to learn more.

GE HealthCare

GEA35693 (5/2025)
JB32544XX