Cybersecurity

Care that's seamlessly connected and continuously protected

gehealthcare.com

Hospitals face a constant and evolving cyber threat landscape. The healthcare industry is spending more time, effort and money than ever to combat costly and potentially dangerous data breaches and cyber attacks.[1]

GE Healthcare helps protect you and your patients through a holistic approach to security. We focus on more than implementing security controls in the devices we make. We continuously work together with our customers and colleagues – across our company, across the healthcare industry and across the cybersecurity field. Because today's hospital is increasingly interconnected, and threats continue to evolve.

At a high level, we focus on two key security program components:

1

Hardening the medical devices

making sure that every device is secured against potential nefarious activity

2

Maintaining security through the lifecycle of our products

assessing and addressing new vulnerabilities as they come out

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 mitigate risks based on the product function and user environment.

DEPS

Design Engineering Privacy and Security is our secure product design and development process. A rigorous set of principles guide us through all stages of product development, testing, and preparation for the market. The DEPS principles include:

- Security control design based on product functionality, considering how the product is going to be used and the environment in which it will operate.
- Threat assessment as a formal input to security controls.
- Threat and risk-based design and implementation of security controls with formal development checkpoints in addition to standard security development best practices.
- Rigorous testing in the later stages of the development cycle. Manual review, vulnerability scans, static and dynamic code analysis, and several phases of internal and external penetration testing are performed and findings addressed.

[1] https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/

We employ experts in medical device cybersecurity

Medical devices, due to their unique capabilities and function, have a different set of security considerations than standard networked IT equipment. That's why GE Healthcare has a dedicated team of cybersecurity experts specialized in medical device security.

Security controls

Protect your organization from the very start.

Preventing breaches begins with building strong cybersecurity controls into our imaging devices and securing new products by design the day they arrive at your hospital.

GE Healthcare embeds a set of security controls* and features into many new products without interfering in the care patients receive. Here's how we help prevent some of the most common cybersecurity risks.

Controlling access

- **Preventing unauthorized access:**
  - Password-protected user access based on role that allows only the minimum access needed for the job.
  - Can be centralized and integrated with your hospital's single sign-on process.
- **Keeping data where it belongs:** USB / DVD export to media can be disabled.
- **Leaving a trail**: Security logs for investigations.
- **Protecting patient data:** Ability to encrypt data moving from your scanner to your PACS.
- **Physically protecting hardware:**
  - Secured with locking doors.
  - Requiring special tools to remove storage.
- **Secure data wipe**: Data can be rendered unreadable and unrecoverable (for asset disposal).

Minimizing vulnerabilities

- **Reducing what can be attacked:**
  - Only-what's-needed software set (no web browser, email client, etc.).
  - Fewer programs means fewer potential footholds for a would-be attacker.
- **Allowing connection only to certain devices** via integrated firewall.
- **Helping to ensure maximum security against external threats:** integrated anti-virus protection.
- **Continuously evaluating and implementing new security patches** while minimizing workflow impact.

* Please note these are just a handful of security controls, this list is not meant to be exhaustive.
Not all of these controls are available in all our products. Please consult the product security manual.

Cybersecurity throughout the lifecycle of the product

Cybersecurity threats are ever-changing and require a vigilant response. We strive to provide fixes to prevent ransomware threats and other attacks before they become a real problem for our customers. We monitor threats as they arise, including vulnerabilities that may apply to our products. We rapidly communicate essential information to our customers, including how to remediate or mitigate emerging issues.

Ongoing cybersecurity maintenance with Continuity

Continuity™ provides added protection throughout the medical device lifecycle.

Available as a separately purchasable option to a service contract, Continuity provides ongoing operating system updates, system software upgrades, and cybersecurity patches to help ensure your devices stay current.

Continuity helps ensure operating system vitality. You will have a supported and patchable operating system, mitigating ever-evolving threats and vulnerabilities. If your OS reaches end of support, GE Healthcare will upgrade the OS to ensure the system is supported.

Continuity

	Continuity Advance	Continuity Support Plus	Continuity Support	Continuity Protect	No Contract
Safety FMIs Field modifications that are required by the FDA due to patient safety	➦	⚙	🛠	🔒	🛡
OS obsolescence protection If the OS reaches end of support, GE will upgrade OS to ensure the system is on a supported OS	➦	⚙	🛠	🔒	
OS updates (installed) GE-validated patches to the operating system to mitigate cyber security risks	➦	⚙	🛠	*	
System software updates Updates to the application software to optimize the performance of the device	➦	⚙			
System software upgrades Application software upgrades to the latest software release (includes computer hardware upgrade if necessary)	➦				

Not all Continuity offerings are available on all GE devices. For diagnostic imaging, GE Healthcare only offers Continuity Advance. Ultrasound offers Continuity Protect, Continuity Support, Continuity Support Plus and Continuity Advance; Life care solutions offers Continuity Protect, Continuity Support and Continuity Support Plus

* Continuity Protect provides OS updates, but customer is responsible for the installation

GE Healthcare reserves the right to make changes in specifications and features shown herein, or discontinue the product described at any time without notice or obligation. Contact your GE Healthcare representative for the most current information. GE, the GE Monogram, and Continuity are trademarks of General Electric Company. GE Healthcare, a division of General Electric Company. GE Medical Systems, Inc., doing business as GE Healthcare.