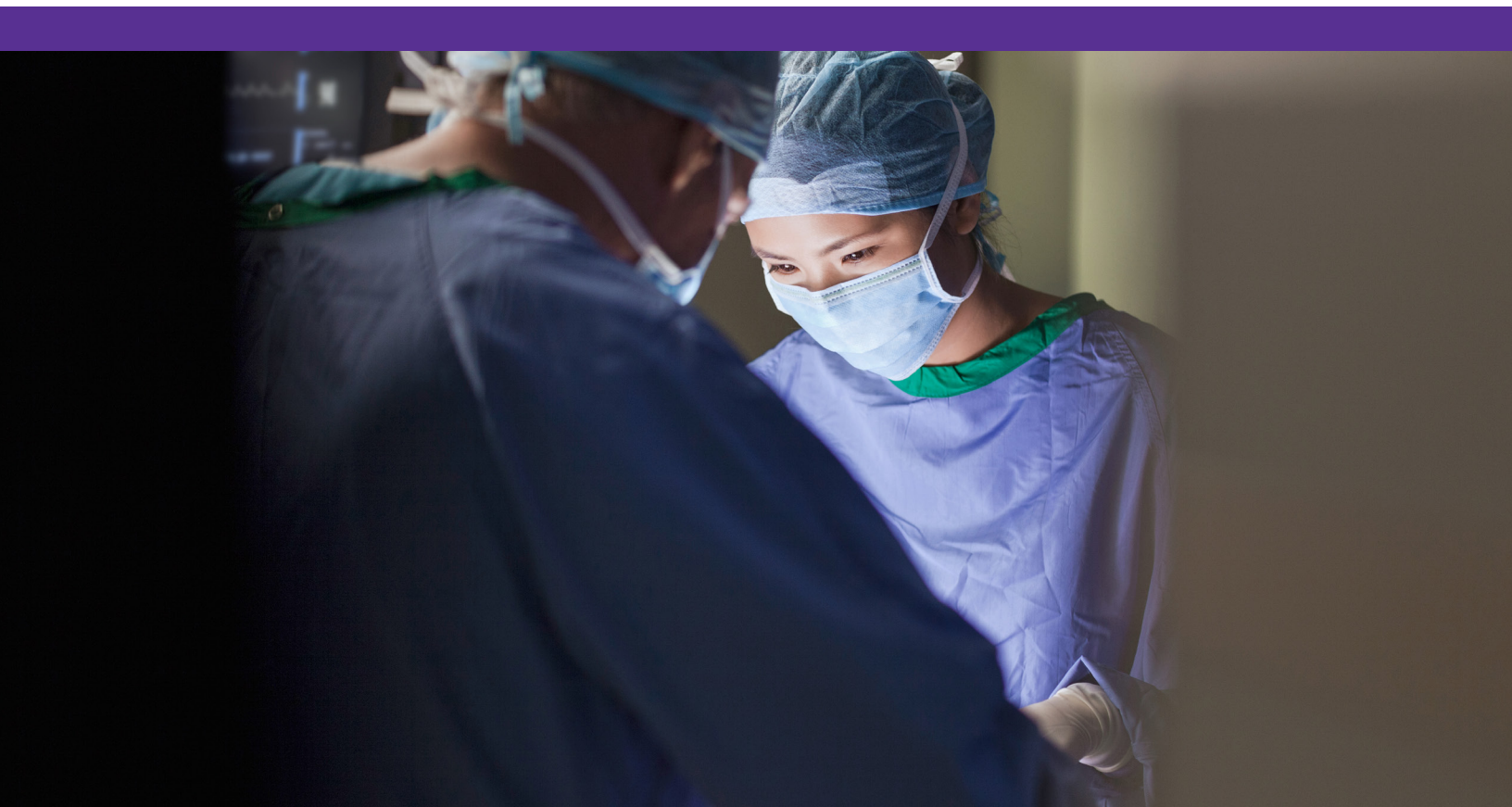




# Secure

## Networked Device Risks and Managed Cybersecurity Services Program

The pace of evolving digital threats targeting health systems and medical technology continues to rise alarmingly. GE HealthCare Secure brings depth of experience, continuous R&D, and collaboration to take on the challenge. We work side-by-side with your information and security leadership to implement strategies that are unique to medical technology, interweaving them into day-to-day security operations. Our Managed Cybersecurity Services program is complementary to any appliance you may have deployed in your ecosystem today for a truly vendor agnostic solution. Proactive monitoring, compliant remediation, active threat scouting and safe integration of AI are just a few examples of what you can expect.



# Skeye

Managed cybersecurity solution for networked medical and IoT devices

**Cybersecurity requires a new approach. But there are ways you can prepare to protect.**

GE HealthCare's Skeye™ solution aligns with the best practices and guidelines of the National Institute of Standards and Technology's (NIST) cybersecurity framework, which is a prioritized, flexible and cost-effective approach to help promote the protection and resilience of critical infrastructure.<sup>1,2</sup> All while leveraging your appliance of choice for a truly vendor-agnostic program.



## Secure features

Skeye leverages medical device expertise, advanced technologies, artificial intelligence and strategic, systematic processes to help keep your network resilient in the face of cybersecurity risk.

### Robust

GE HealthCare's managed cybersecurity services for networked medical devices are designed to help assess, understand, protect, facilitate remediation and support cybersecurity efforts.

### Dedicated

GE HealthCare's dedication to cybersecurity is backed by a proactive MedTech Security Operations Center (SOC) responsible for monitoring an organization's networked medical device inventory—as well as detecting, analyzing and responding to security vulnerabilities in real-time.

### Inclusive

By design, GE HealthCare's cybersecurity approach helps ensure that all networked medical devices within an organization receive the same high level of protection, regardless of age, OEM or operating system.

### Experienced

A leading provider of medical technologies, digital infrastructure and data analytics solutions, GE HealthCare is a beacon in the medical device protection and cybersecurity space. And because GE HealthCare is a multi-vendor service provider, customers can also depend on this same expertise to help protect their inventory of networked medical devices—regardless of manufacturer.

# Proactive protection. Total peace of mind.

## Managed Cybersecurity Services Program

Today, patient care depends on the interconnectivity of hundreds of medical devices. All of which must be carefully cataloged and monitored. But with more and more medical devices—connected to more and more networks—cybersecurity threats start to become real. Managing risk at every end point has become more important than ever before.

- More than 93% of healthcare organizations experienced a data breach in the past three years.<sup>3</sup>
- The average cost per healthcare record breached increased from \$429 in 2019 to \$499 in 2020.<sup>3</sup>
- Healthcare data breaches increased 55.1% from 386 in 2019 to 599 in 2020.<sup>3</sup>
- This cost healthcare organizations around \$13.2 billion in 2020.<sup>3</sup>

## Security Operations Center

At GE HealthCare, MedTech Security Operations Center (SOC) is at the heart of our cybersecurity environment. Our SOC uses sophisticated technologies and artificial intelligence for automated, end-to-end security protection.

- Professionals with cybersecurity and medical device expertise
- Helps detect, analyze and respond to cybersecurity threats in real-time
- Incorporates artificial intelligence tools for greater insights and faster response times

## Secure differentiators with MTAS

### 1 Integrated service

Integrates into your Services delivery program for management of remediation plans.

### 2 Proactive approach

Provides scouting and vulnerability research proactively to health systems.

### 3 Flexible solutions

Works with your health system's current appliances and security infrastructure by bringing managed security services resources, processes and proprietary monitoring technology.

### 4 Vendor agnostic

Agnostic view across your health system's programs for planning and deployment of upgrades, network change requirements, installations and other changes to medical devices.

1. <https://www.nist.gov/cyberframework>

2. Applies only to medical devices under GE HealthCare service contract.

3. [beckershospitalreview.com/cybersecurity/healthcare-data-breaches-up-55-1-in-2020-report-finds.html](https://beckershospitalreview.com/cybersecurity/healthcare-data-breaches-up-55-1-in-2020-report-finds.html)

