PHILIPS

Service and solutions delivery

Cybersecurity services

Securing medical devices, systems, and networks

Securing medical devices, systems, and networks

Philips Cybersecurity services are designed to safeguard medical devices and to assist in compliance with the rigorous requirements of federal, state, and local government standards.

The proliferation of millions of connected medical devices allows users to share, search, navigate, manage, and analyze the limitless flow of data that enhances care outcomes. Connectivity plays a transformational role in healthcare and exposes patients and organizations to safety and security risks. Assuring the safety and privacy of these devices, systems, and their associated data requires a comprehensive risk-based cybersecurity program.

Healthcare data is the #1 target for cybercriminals and is ten times more valuable than credit card data alone (HHS Report, April 12, 2018). Threats include malicious security attacks via viruses, worms, and hacker intrusions. According to the 2020 Protenus Breach Barometer report, there were 572 healthcare data breaches of 500 or more records in 2019 and at least 41.4 million patient records were compromised. This disturbing trend has forced executives to consider medical device security as a significant risk facing healthcare today.

> *"Data is the new currency, and hacking is a business model. The financial gains of hacking will soon surpass those of the worldwide drug trade."*
>
> Stef Hoffman, Chief Information Security Officer, Philips

Ransomware puts patient safety at risk

In September of 2020, thirty servers at a major hospital in Dusseldorf, Germany, were suddenly encrypted and forced offline. As systems crashed and access to data was compromised, emergency patients were redirected, and operations were postponed. In one instance, a woman requiring urgent admission died after being transported 20 miles to another facility. It was the first time a ransomware attack was directly attributed to the death of a patient*.

Investigators suggest the hacker exploited a weak spot in a "widely used commercial add-on software." This attack is reminiscent of the WANNACRY attack on the British NHS that forced several hospitals to divert patients.

*https://www.independent.co.uk/wires/us/german-hospital-hacked-patient-taken-another-city-dies-b472963.html

A comprehensive approach

Maintaining and securing a hospital-wide network of connected medical devices and software is critical to the ongoing safety of patients, not only physically, but from an identity theft perspective. However, there is no one-size-fits-all solution – no out-of-the-box product that is capable of performing effectively to sustain security in the face of growing risk. Effective medical device cybersecurity must be strategic and comprehensive. Philips provides an end to end security offering, which complies with and builds upon global regulations to make medical devices, systems, and networks robust against cyber threats.

To be successful, the commitment to managing effective cybersecurity must also be horizontal. Healthcare providers must break down silos to forge an ongoing collaboration between operations and technology personnel, hospital-wide. Security must become part of the institutionalized culture, integrated holistically.

> *"There is no one golden solution. We have to embrace security and privacy in our organizations. Every one of us within this ecosystem needs to play our role in mitigating the threat."*
>
> Gal Gnainsky, Head of Philips Group Security

Relationships and collaboration are key

In an ecosystem composed of multiple stakeholders – industry regulators, healthcare leaders, clinicians, patients, and manufacturers of health IT equipment – each party has a role to play. By collaborating across this healthcare ecosystem, the industry can build on advances made by other critical infrastructure industries, supporting the advantages that digital connectivity brings to patient care. Healthcare providers then benefit from this unified approach by applying learnings and best practices.

Philips is well-positioned to engage with healthcare providers in a cybersecurity partnership designed to employ comprehensive cybersecurity risk management strategies across the enterprise. The company brings its 'security designed in' mindset to every engagement. This systemic approach begins with product design and development and is carried through testing and deployment – followed up with robust policies and procedures for protection, updates, and monitoring – and when necessary, incident response management, remediation, and recovery. The company chartered its Product and Solutions Security Program to create, implement and update practical approaches to meet customer requirements, and the Philips Security Center of Excellence shares information with leading cybersecurity researchers and test facilities around the world, assisting them to educe and eradicate cyber threats quickly.

Philips Cybersecurity services are customer offerings that are tailored to define a specific set of solutions to maintain proper security postures over time for a robust and reliable security profile. The intent is to establish a mutually beneficial partnership that will deliver positive, sustainable results.

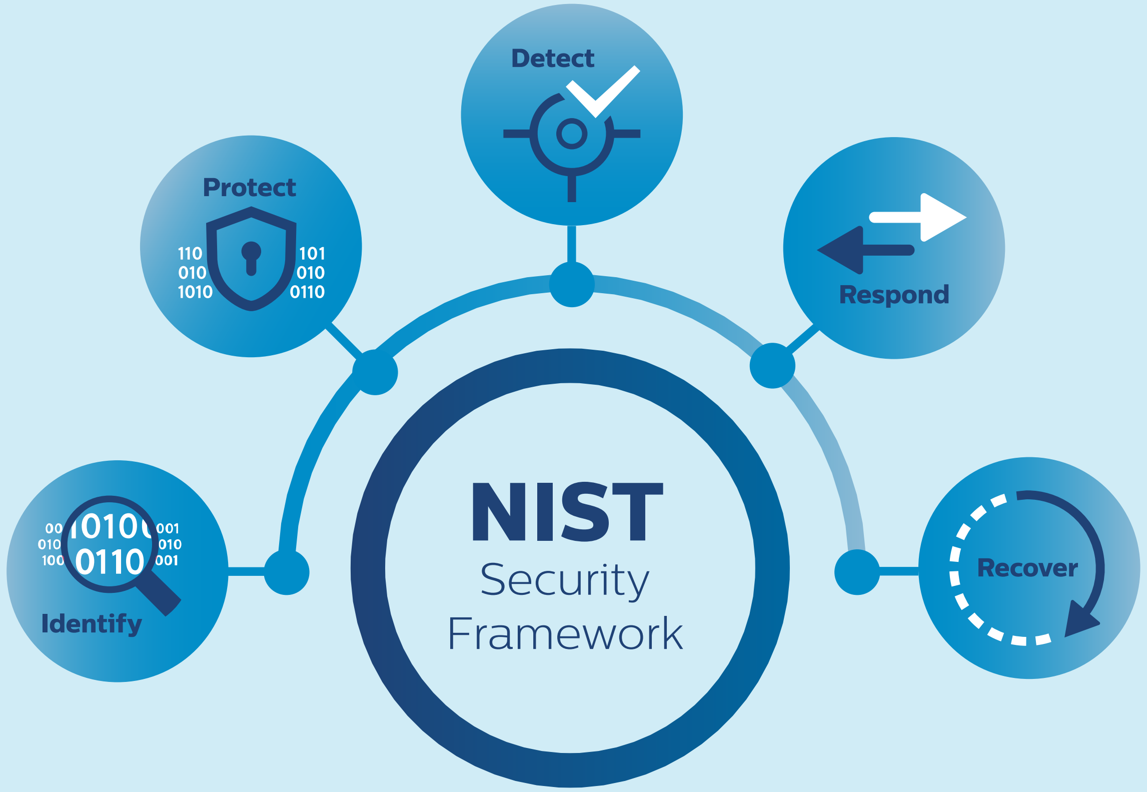
Program essentials

Philips Cybersecurity services is a suite of technologies and services designed to safeguard medical devices. These solutions align with global cybersecurity best practices and are based on the NIST cybersecurity framework. Services are customized to individual requirements and cover:

- Security maturity assessment
- Regulatory compliance
- Periodic patching
- Legacy system upgrade and protection
- 24/7 asset monitoring
- Security threat assessment and tracking
- Response and recovery procedures
- Access authentication and audit logging

As the partnership between Philips and the customer matures, services are easily adjusted to reflect a new security posture.

National Institute of Standards and Technology (NIST) cybersecurity framework



Identify
Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities

Protect
Develop and implement appropriate safeguards to ensure the delivery of critical services

Detect
Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event

Respond
Develop and implement the appropriate activities to take action regarding a detected cybersecurity event (SOC)

Recover
Develop and implement appropriate activities to maintain plans for resilience and to restore any impaired capabilities or services due to a cybersecurity incident

Philips Cybersecurity services are designed specifically for the healthcare ecosystem to address the complexities customers face due to the wide variety of medical devices they are required to secure. Having the knowledge, resources, and competencies to validate and verify enables Philips to create a robust response.

A full set of cybersecurity services:

Philips Cybersecurity Consulting
Security consultants help customers with risk and vulnerability assessments of medical systems, regulatory compliance, and advice on implementing organizational processes that seamlessly integrate security response and recovery workflows across all suppliers. By delivering this support, hospital staff can focus more closely on patient care than on the immense task of securing medical devices.

Philips Cybersecurity Protection and Upgrade Services
Technology and services are used to keep customer systems secure through coordinated vulnerability disclosures, medically validated OS patching, a software upgrade to the latest security level, and network segmentation. Also, with an upgrade and mitigating controls such as network segmentation, these services will help customers maximize the lifetime usage of their medical devices. Philips helps find the perfect balance between security protections required and the downtime caused by the medical validation of those controls.

Philips Cybersecurity Detection and Recovery Services
Technologies are employed to help customers identify their medical assets, and monitor the security posture of their medical systems 24/7 and, where needed, trigger response and recovery workflows, as well as assist in recovery from cybersecurity attacks. Philips identifies incidents with specific healthcare context to avoid data overload and then closes the loop with remediation efforts, allowing healthcare providers to resume operations as soon as possible.

Philips Cybersecurity Access and Audit Services
These services are designed to support customers to maintain control over who (vendors and employees) access their systems and allow for streamlined/compliant auditing of procedures and data. Being able to gain an overview of who has access provides essential insights into a hospital's security profile – indicating strengths and possible vulnerabilities.

> *"Philips provides a stream of cybersecurity services that enable customers to mature and continuously progress within their cybersecurity program with the focus of securing medical devices and systems and the boundaries of the networks that they sit on."*
>
> Jonathan Bagnell, Cybersecurity Global Market Leader, GS Product Security & Services

Partnered for best-in-class medical device security

To effectively protect connected medical devices, the ability to identify and assess all of them (regardless of vendor) is critical. In many hospitals, the number of devices can run into the thousands.

Philips has partnered with CyberMDX, a leading healthcare cybersecurity provider that delivers visibility and threat prevention for medical devices and clinical networks. CyberMDX provides technology that protects connected devices in a hospital environment, whether managed or unmanaged, by leveraging a combination of risk assessment, detection, threat intelligence, and prevention capabilities.

CyberMDX performs a risk assessment for the entire network of connected devices to:

Identify
Continuous discovery and classification of all IoMT, IoT, OT assets

Assess
Healthcare-context risk assessment, security insights, and remediation plan

Detect and Prevent
Anomaly and malicious activity detection; preventive measures to reduce the attack surface

Data and insights analyzed through CyberMDX serve as the basis for the development and implementation of a full cybersecurity plan for the individual healthcare provider. Moving forward, it also allows Philips, and the customer, to sustain a proactive position in the ever-evolving cybersecurity environment.

> *"On-premises connected medical devices are 'extremely vulnerable' to being hacked or held for ransom. Some were built without security in mind, some suffer from broken post-market security processes. Now, they are exposed to a much higher risk, as the chances an intruder will get into the network become higher."*
>
> Motti Sorani, CTO of CyberMDX

People, processes, and technology drive the program

Philips Cybersecurity services embody Operational Intelligence – a new way of working that merges skills and capabilities. Operational Intelligence is a partnership of continually synchronized people, processes, and technology. Philips finds that this approach offers cumulative gains, unlocking not only hard value but also the softer, more people-powered value that is difficult to quantify, but which delivers significant benefit. In cybersecurity, it is this aspect that differentiates the Philips offers.

Philips solutions encompass providing on-site BioMed, IT, compliance and security people backed by Philips Group Security processes and enabled by technology selected explicitly for healthcare.

As an example, consider the following framework:

On-site dedicated BioMed and security team

- Security officer
- DPO / Compliance officer
- IT Director
- Transformation manager
- Project manager(s)
- Service account manager

Backed by Philips Group Security processes

- Assess security vulnerabilities
- Provide risk management advice
- Assure 24/7 incident response and remediation
- Deliver monthly threat reports

Enabled by technology selected for healthcare

- Automated inventory and incident detection
- Automated security configuration management
- Uniform remote service access management
- Legacy management via OS upgrades

The close integration between people, processes, and technology allows Philips to present a comprehensive cybersecurity package – one that reflects the broad experience of a global cybersecurity leader.

Meeting and exceeding security standards

Philips also takes the lead in collaborating with regulatory agencies such as the FDA and international regulators (via HIPAA, ASIST, HITRUST, GDPR), industry partners, and healthcare providers to implement the latest safeguards. Philips product security risk assessments are aligned with several standards, including the FDA recommended ISO/IEC-800001 standard, NIST 800-53 Rev 4, ITIL v3.1.24, ISO/IEC-27000 series standards, ISO 14971, EU Directive 95/46/EC, and HIPAA Security and Privacy Rules. In 2020, Philips was ranked #1 in a group of similar cohort companies by BitSight Security Ratings – a data-driven and dynamic measurement of an organization's cybersecurity performance that is both material and validated.

In December 2019, Underwriters Laboratories (UL) launched a new security option for their IEC 62304 Registered Firm certification program. This option is designed to evaluate the internal capability maturity of a medical device manufacturer to test the robustness of their products' security controls, using the tests of UL 2900-2-1 Software Cybersecurity as part of their IEC 62304 Medical Device Software Life Cycle Processes. Philips is the first medical device manufacturer to exercise this new option for demonstrating their internal security testing capability maturity.

A scalable solution

It is important to emphasize that this cybersecurity offering is fully scalable and customizable. Some healthcare providers may require only an assessment and analysis of their current security protocols; others may determine that a complete end-to-end solution offers the best protection profile. Still others can choose the service(s) that meet their unique needs.

Technologies that provide security data are essential. However, it is the ability to use that data and continuously verify and validate it, as well as take it and report it up into a level of security metrics that are actionable by the healthcare provider, which is critical.

The deployment of a successful cybersecurity program is achieved by being diligent in applying policies and procedures across people, processes, and technology. This inclusive approach ensures security excellence and continuous improvement. It is an example of the industry expertise that differentiates Philips Cybersecurity services.

The services will only be available for delivery in NAM market in 2021 for selected Philips modalities.

4522 991 64501 * NOV 2020

How to reach us
Please visit www.philips.com
healthcare@philips.com