PHILIPS

Philips and cybersecurity

Committed to proactively addressing our customers' security concerns

Position paper | June 2025

Table of contents

The digitalization of healthcare – opportunities and threats	3
Philips position on cybersecurity	4
Transparency, compliance and beyond	5
Product security	6
Enterprise information security	8

The digitalization of healthcare – opportunities and threats

Today's healthcare systems are faced with the challenges of an aging population and the rising incidence of chronic diseases. Additionally, the industry is struggling to develop appropriate and affordable care models. Connected healthcare – enabled by devices, health apps, and platforms – has unprecedented potential to transform healthcare, and enable better health and better care at a lower cost.

The proliferation of millions of connected digital devices allows users and networks to share, search, navigate, manage, compare and analyze a virtually limitless flow of data that can be used to enhance care outcomes.

This digital 'ecosystem' has already helped the industry expand the personal and healthcare-oriented smart devices portfolio, sparked innovation, and increased service efficiency.

For example, analysis of electronic medical records and diagnostic information gathered by imaging equipment, monitors and handheld personal devices enhances the decision-making powers of professionals and enables people to take a more active role in managing their health.

However, the exponential growth in the volume and types of data also leads to increased vulnerability to cybercrime. Over 90% of global healthcare organizations have reported at least one security breach within the last few years.[1] Additionally, a data breach in healthcare results in higher monetary damages than any other industry, with the average breach costing USD 9.77 million.[2]

The personal data in healthcare records is particularly valuable, as it can be used for a range of malicious purposes, such as identity theft and insurance fraud.

Threats to healthcare institutions include malicious security attacks via viruses, worms and hacker intrusions. Perpetrators range from attic-room hackers to organized crime and even nation-states.

The global, exponential rise of ransomware attacks shows that even the largest and most sophisticated organizations can be vulnerable to disruption. In these cases, some hospitals have had to divert patients to other clinics.

Remote working and e-commerce, which saw exponential growth during the COVID-19 pandemic, has brought about a host of new cyber challenges.

"Security is job zero."

Shez Partovi
Chief Innovation & Strategy Officer, Philips

[1] Palatty, 80+ Healthcare Data Breach Statistics 2024, Astra, February 6, 2025.
[2] IBM, Cost of a Data Breach Report 2024.

Philips position on cybersecurity

Philips delivers innovations that help consumers and healthcare professionals connect more easily and make better-informed decisions. Some of the most powerful and promising opportunities for these innovations involve research into large study groups and big data sets.

Keeping that information secure is a key priority for Philips, as our strategic and competitive positions rely heavily on data, digital innovation and consumer trust. Quarterly reporting drives the priorities and risk appetite for the security domain with recommendations from our security department, audit findings and other appropriate contributions.

Recognizing the concerns of our customers and consumers, and the critical role security plays across today's interconnected digital ecosystems, Philips is committed to the deployment of a comprehensive security strategy that assures the safety of product, business (enterprise information) and personal (patient) data.

Our security strategy – which we refer to as 'secure by design' – encompasses our people, processes and technologies. The goal of this approach is to ensure the confidentiality, integrity and availability of critical data and the systems where data is stored.

Secure by design is an integrated approach in which security is top of mind as systems and their components are built. In this way, health information and medical devices are protected and secure throughout their entire lifecycle.

Security – like safety and quality – is a prerequisite for confidence in the Philips brand. Customers and consumers must be able to rely on the security, safety and quality of our products and services. Therefore, we continue to be proactive in highlighting the benefits of connected healthcare technologies and continue to invest in secure systems that customers can rely on.

"Philips helps healthcare providers focus on patient care in a secure way. Partnerships are key for achieving seamless and secure services in this complex, rapidly-growing ecosystem."

Gal Gnainsky
Chief Security Officer, Philips

Transparency, compliance and beyond

Philips implements security within a heavily regulated medical device industry. Regulatory agencies and policies, such as the United States Food and Drug Administration (FDA) and the European Union Medical Device Regulation (EU MDR), require that hardware and software releases and changes be subjected to rigorous verification and validation methods to assure that high standards of safety, security, efficacy, quality and performance are met in all applicable Philips products and services.

Philips strives to be open and transparent in reporting and remediating vulnerabilities and has developed a robust Coordinated Vulnerability Disclosure process.

Our strategy involves staying on top of emerging security vulnerabilities and potential external threats, and collaborating with regulatory agencies, industry partners, and healthcare providers, among others, to close security loopholes and implement safeguards.

Philips actively participates in key industry groups that have a security or privacy focus to further align our efforts. We strive to ensure that the appropriate and necessary customer security requirements are included in industry standards, guidelines and initiatives.

We were a charter member of the US Department of Health and Human Services (HHS) Cybersecurity Taskforce that delivered a report illustrating the urgency and complexity of cybersecurity risks that the healthcare industry is facing – an effort that continues to influence industry working groups. We are strongly involved in the development of healthcare security standards through several standards development organizations, including the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

"By partnering with our customers and being transparent, we keep evolving the security of our products and services, with the goal of ensuring patient safety."

Dirk de Wit
Head of Product Security, Philips

Product security

Philips takes the growing risk of cybersecurity threats to our products seriously. Our security-first approach continues to drive our commitment to improving our processes and systems to minimize the risk to the patients who depend on our solutions and services.

We are keenly aware of the growing trend of sophisticated cyberattacks across industries and increasingly in healthcare. The potential impact of cybersecurity vulnerabilities continues to grow as hospital networks, clinical databases, medical devices and personal health monitoring systems become more integrated.

Philips was an early leader in recognizing that effective cybersecurity is no longer about protecting the 'box' or an individual product – it requires a systematic approach that considers where and how devices are employed. As such, we implemented a coordinated vulnerability management process three years prior to industry-wide adoption of Coordinated Vulnerability Disclosures (CVD). Additionally, Philips became the first medical device manufacturer to achieve a UL2900 certified for excellence in security testing in 2019.

The Philips Product Security department governs the embedding of security into all products and services during the entire lifecycle, through a product security framework – part of the Philips Excellence Framework. The security framework includes product security risk assessments, independent vulnerability and penetration assessments, specialized product security trainings, and response activities for vulnerabilities identified in existing products and services that are under maintenance and support contracts.

At Philips, secure by design is an end-to-end mindset that infuses security principles and begins with product design and development through testing and deployment. This approach is supported with robust policies and procedures for monitoring, effective updating, and managing incident responses.

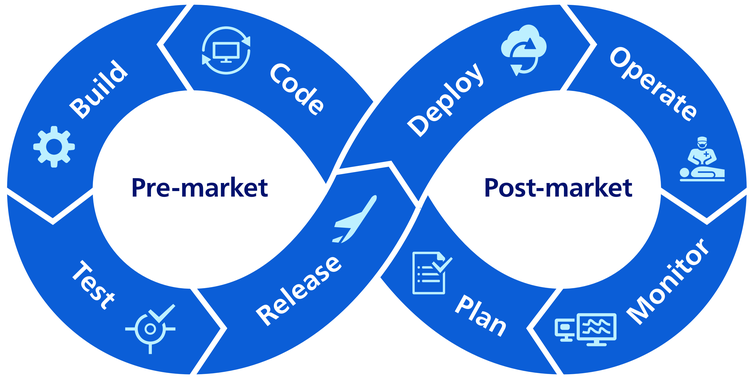
To make our products and services robust against cyber threats requires an unwavering commitment to risk assessment and adherence to security-based product development. It requires the fast deployment of security-enabling technologies (such as encryption and patch management) and continuous improvement. That is why we have chartered our Product and Solutions Security Program to create, implement and update comprehensive and practical approaches to meet customer requirements.

Key Philips product security initiatives include:

We adhere to an industry-advanced Philips Product Security Policy, consisting of policies, procedures and timely documented actions empowering the organization to implement security best practices.

The policy outlines our strategic organization and procedures for:

- Maintaining a global network of security professionals.
- Governing threat modeling activities to proactively assess potential threats when new product developments start.
- Developing and deploying best practices for our products and services.
- Governing risk assessment activities related to potential security and privacy threats as well possible vulnerabilities.
- Guiding incident response activities related to identified security and privacy threats.
- Governing security embedded in products and services during their lifecycle.
- Supporting our HealthSuite platform to align to the latest security standards for cloud environments.
- Continuously monitoring for vulnerabilities and validating fixes as part of our Secure Product Development Lifecycle – activities that are supported by our internal Security Center of Excellence.



Philips' Security Center of Excellence shares information with leading cybersecurity researchers and test facilities around the world, to help them rapidly eliminate, reduce and mitigate cyber threats.

Implementation of security standards that meet or exceed current regulatory requirements and industry best practices, including:

- Product security requirements for products and services that are aligned with regulatory recommended standards and used as the basis for the 80001-2-2 standard.
- Services security aligned with recognized standards such as NIST SP 800-53, ISO/IEC 27000 series and HITRUST.
- Creation of customer-facing information, such as the industry-standard Manufacturer Disclosure Statement for Medical Device Security (MDS).
- Support for FDA, EU MDR and other laws and regulations that address cybersecurity in medical devices.

The Philips Security Center of Excellence has undergone a comprehensive audit by UL Solutions as part of its registration for the IEC 62304 security option. The audit reviewed and verified core Philips Security Center of Excellence product security processes, including security risk management and risk control measures, software security verification planning, change management and continuous improvement, and the center's laboratory quality management system.

Monitoring and responding to threats, vulnerabilities and security incidents

- Philips continually monitors for new security threats, vulnerabilities and security incidents, including those identified by the operating system and by third-party software vendors, customers and security researchers.
- Philips Product Security Incident Response Teams evaluate potential security incidents and vulnerabilities, and develop response plans as necessary.

Malware protection and patch management

- Products that support commercially available malware protection may be delivered with pre-installed malware protection software or customer documentation, detailing product-specific, Philips-approved malware protection parameters.
- Philips products might use third-party software, including operating systems such as Microsoft Windows and Linux. Impact assessments of their hotfixes by Philips product engineering teams typically begin within 48 hours of Philips' awareness of a new security vulnerability or patch availability.
- Philips deploys a variety of programs to address lifecycle cybersecurity risks, including a range of services that guard against threats related to obsolescence of platforms and devices.

Reporting and addressing identified vulnerabilities

- We have designed and implemented a CVD, which has been singled out as a best practice in the industry.
- Our CVD policy is publicly accessible, with clear communications channels for customers, researchers and other security community stakeholders.
- The policy encompasses monitoring of and response to inbound communications, follow-up engagement, evaluation of vulnerability notifications and status tracking, and alignment with incident response, remediation and prevention policies.
- We are a Certified Numbering Authority (CNA) that can publish identifiers for Common Vulnerabilities and Exposures (CVE), which enable coordinated, industry-wide efforts to address software security flaws.

Philips is committed to ensuring the security of our medical devices through long-term strategic and effective innovations.

Product security continues to be a critical challenge in the healthcare industry and we look forward to driving conversations forward as part of our goal to improve billions of lives worldwide.

Enterprise information security

Philips' growth is fueled by innovative technologies that our customers have grown to trust and rely upon. Sophisticated internal information systems support the design, development and production of these technologies.

The goal of the Philips information security organization is to safeguard enterprise information systems. Rapidly growing cybersecurity threats target these technologies and the data housed within, meaning we must work to ensure:

- **Our customers' trust**: enhance the Philips brand to be synonymous with safety, quality and security
- **Our ability to grow**: prevent the loss of proprietary information to ensure the company's long-term competitive future
- **Our financial performance**: protect enterprise assets to prevent negative financial impacts, including loss of customers, revenue and profit
- **Our operational stability**: maintain continuous operation by preventing the degradation or disruption of vital infrastructures
- **Our compliance to regulations**: Philips assesses against industry best practices and the latest regulatory requirements (e.g., NIS2, CRA, FDA, NMPA, ISO) and continuously improves key security controls (e.g., strengthening endpoints, email security and network security, and conducting global vulnerability scans, including mitigation of vulnerabilities)

Information security cannot be solved through technology alone. Comprehensive information security requires focus on three domains: people, processes and technology. The Philips Information Security organization implements controls across these domains to facilitate the following:

- **Confidentiality**: only those who should have access can retrieve data
- **Integrity**: information cannot be modified without detection
- **Availability**: information can be accessed when needed

Philips is meeting – and will continue to meet – the challenges of an evolving threat landscape to secure enterprise information systems and increase customer trust. The Philips Information Security organization is committed to focusing investments on retaining top-tier cybersecurity talent, enhancing cybersecurity tooling and capabilities, and integrating security best practices in everything we do.

Information security focus on people, processes and technology

People

Focuses on the behavioral aspects of employees and improves their security aptitude, thereby developing a security culture

Processes

Focuses on our business processes and ensures security risk is evaluated, and proper mitigation steps are integrated into our processes to reduce that risk

Technology

Focuses on understanding and monitoring our technology landscape and making technological improvements to enhance our security risk posture

On a societal level, cybersecurity resilience has been elevated to a critical concern resulting in a growing number of detailed regulations. These regulations not only cover products and services, but the company that provides these products and services. We at Philips are cognizant of our role and responsibilities as part of our customers' supply chains, as well as our responsibility for our own supply chain.

"Information security, like quality, must be embedded in our DNA and integrated into everything we do."

Wim Sonnemans
Head of Information Security, Philips

www.philips.com