PHILIPS

Position paper

Philips and cybersecurity

Committed to proactively addressing our customers' security and privacy concerns

January 2018

Table of contents

"Cybersecurity is front and center in the transition to connected care"

Jeroen Tas
Chief Innovation & Strategy Officer, Philips

1. The digitalization of healthcare – opportunities and threats

Faced with the challenge of an aging population, today's healthcare systems are struggling to develop appropriate and affordable care models. Connected healthcare – enabled by connected devices, health apps and platforms – creates an unprecedented potential to transform healthcare and enable better health and better care at 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 portfolio of personal and healthcare-oriented smart devices, sparked innovation, and increased service efficiency.

As an example: analysis of electronic medical records and diagnostic information gathered by imaging equipment, monitors and hand-held personal devices enhances the decision-making powers of professionals and enables a more active role for people to manage their personal health.

However, the exponential increase in the volume and types of data available also leads to increased vulnerability to cybercrime – healthcare data is the #1 target for cybercriminals and is 10 times more valuable than credit card data alone.

Personal data within healthcare records is most valuable, as it can be used, for example, for various malicious purposes such as creating false identities or making false insurance claims.

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

Cyber-attacks such as the WannaCry ransomware attack in May 2017 show that even the largest and most sophisticated organizations can be vulnerable to disruption. In this case, some hospitals even had to divert patients to other clinics.

>100,000,000
records breached in 2015

34% of records compromised are healthcare-related[1]

Over 75%
of all legitimate websites contain **unpatched vulnerabilities**[2]

Two billion
personal records were stolen in the US in 2016, **100 million** of which were medical records[3]

#1 target

Healthcare is primary target

A healthcare record lost or stolen could cost as much as **$363 per record** to remediate[4]

The cost of
cybercrime
is expected to reach **$2 trillion** by 2019[5]

In 2016, cybercrime cost the global economy upwards of
$450 billion[6]

Sources:
1. IBM X-Force Threat Intelligence Report 2016
2. Symantec
3. CNBC
4. IBM X-Force Threat Intelligence Report 2016
5. Juniper research
6. CNBC

2. Philips' position on cybersecurity

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

Philips' strategic and competitive position relies heavily on **data, digital innovation and consumer trust**.

Philips is handling increasing amounts of health-related data, one of the most sensitive types of personal data. **Our customers are requesting increasingly high levels of assurance regarding the security and privacy protection measures we have in place**. Increasingly our privacy measures are critical in decisions to do business with partners.

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 **comprehensive security plans** that assure the safety of product, business (enterprise information) and personal (patient) data.

Our security plans encompass our **people, processes and technology**, with the goal of ensuring the **confidentiality, integrity and availability** of critical data and the systems that house that data.

The concept of **Security Designed In** (or **Security by design** in the EU) – end-to-end, from design to production to support – is key to the long-term success of our products, services and solutions.

Philips promotes consistent adoption of strategies to proactively address risks and threats, including what are often referred to in the area of cybersecurity as **'The Three Deadly Sins'**:

- **password risk**: the risk from a lack of strong identity and permission management, e.g. multifactor authentication
- **encryption risk**: the risk from a lack of strong end-to-end data encryption – from the source where data is generated, over the network and when resting in a data center – and/or effective data-loss prevention solutions
- **patch management risk**: the risk from a lack of effective patch management, creating vulnerabilities in, for example, legacy operating systems.

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** and see the value of sharing their data – otherwise the health benefits that come from connectivity and analysis of big data sets may never be realized. Therefore, we continue to be proactive in highlighting the benefits of connected health technology and continue to invest in secure systems that customers can rely on.

"Product and information security is a combination of education, policies and procedures, physical security and technology"

Michael McNeil
Head of Global Product & Security Services, Philips

3. Transparency, compliance and beyond

Philips implements security within a heavily regulated medical device industry. Regulatory agencies such as the US Food and Drug Administration 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 ensures **compliance** with data protection and privacy standards and regulations.

Philips strives to be **open and transparent in reporting and remediating vulnerabilities** and has developed a robust Coordinated Vulnerability Disclosure process (previously defined as Responsible Disclosure).

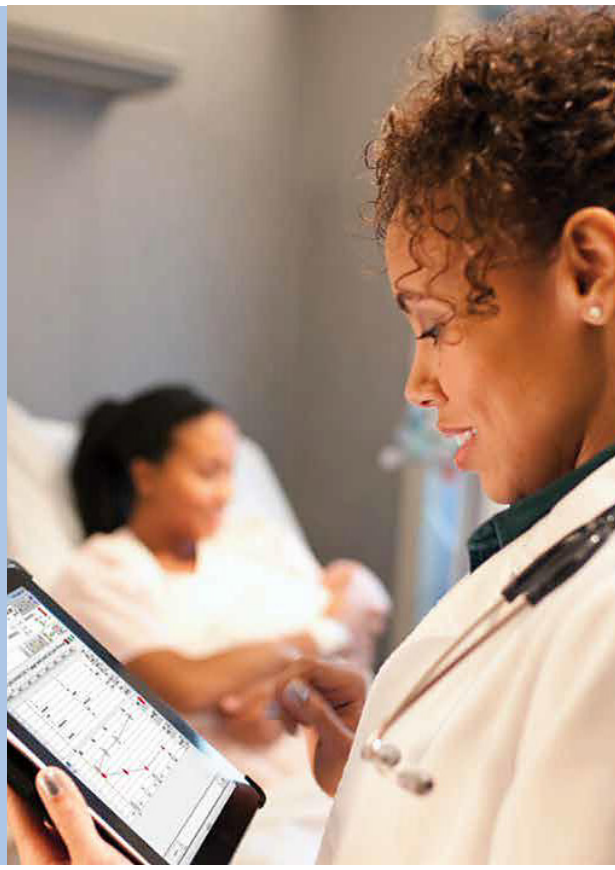
Our strategy involves not just staying on top of emerging security vulnerabilities and potential external threats, but also **taking responsibility and collaborating** with regulatory agencies, industry partners and healthcare providers, among others, to close security loopholes and implement safeguards.

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

Philips supports the **World Economic Forum's** 'Recommendations for Public-Private Partnership against Cybercrime'.

"Patient safety in today's connected care environment is a task we all take very seriously. As we all evolve our cybersecurity programs, transparency, accountability and responsiveness must be priorities we continue to maintain."

Michael McNeil
Head of Global Product & Security Services, Philips



4. Product security

Philips takes the growing risk of cybersecurity[1] threats to our products very seriously. We have long been committed to the ongoing effort to continuously improve 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. As hospital networks, clinical databases, medical devices and personal health monitoring systems become more integrated, the potential for cybersecurity vulnerabilities also grows.

Philips was an early leader in recognizing effective cybersecurity is no longer about protecting the 'box' or individual product, but a systematic approach that takes into account where and how devices are employed. **At Philips, 'Security Designed in' is an end-to-end mindset: infusing security principles begins with product design and development, through testing and deployment – and followed up with robust policies and procedures for monitoring, effective updates, and where necessary, incident response management.**

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 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 effective approaches to meet customer requirements.

Key Philips product security initiatives include:
Launch of an industry-advanced, publicly available Philips Product Security Policy, consisting of policies, procedures, and standards empowering the organization to implement security best practices.

The Policy outlines our strategic organization and procedures for:

- Maintaining a global network of security and privacy professionals operating under the Philips Product Security Policy
- Developing and deploying best practices for our products and services
- Guiding risk assessment and incident response activities relating to potential and identified security and privacy threats and vulnerabilities
- Governing security embedded in product and services during their life-cycle, including risk assessment and response for identified vulnerabilities in products and services

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

- Product security and privacy requirements for products and services which are not only aligned with the FDA-recommended standard ISO/IEC-800001, but were even used as the basis for the 80001-2-2 standard.
- Services security and privacy requirements aligned with recognized standards such as NIST 800-53 Rev 4, ITIL v3.1.24 and ISO/IEC-27000 series.
- Creation of customer-facing information such as the industry-standard Manufacturer Disclosure Statement for Medical Device Security (MDS[2]).
- Support for FDA guidance on Premarket Management on Cybersecurity in Medical Devices, and FDA Postmarket Management of Cybersecurity in Medical Devices.

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

Monitoring and response to threats, vulnerabilities and security incidents:

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

Malware protection and patch management:

- Products that support commercially available malware protection are delivered with pre-installed malware protection software, or with customer documentation, detailing parameters of product-specific Philips-approved malware protection.
- Philips products might utilize third-party software, including operating systems like Microsoft Windows and Linux. Impact assessments of these hotfixes by Philips product engineering teams typically begin within 48 hours of Philips' awareness of a new security vulnerability or patch availability.

A Responsible Disclosure Policy to report and address identified vulnerabilities:

- We have designed and implemented a Responsible Disclosure policy of this kind, which has been singled out as a best practice in the industry.
- Our Responsible Disclosure policy is publicly accessible, with clear communications channels for customers, researchers and other security community stakeholders.
- The policy encompasses monitoring and response of inbound communications, follow-up engagement, evaluation of vulnerability notifications and status tracking, and alignment with incident response, remediation and prevention policies.

Philips is committed to continuing to innovate long-term strategic and effective measures to further instill the ethos of medical device product security. We look forward to continuing this critically important conversation, in order to help meet our goal of improving billions of lives worldwide.

1. Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access - http://whatis.techtarget.com/definition/cybersecurity

"Data is the new currency, and hacking is a business model. The financial gains of hacking will soon surpass those of the worldwide drugs trade."

Stef Hoffman
Chief Information Security Officer, Philips

5. Enterprise information security

Philips' growth is fueled by innovative technology that our customers have grown to trust and rely upon. The design, development and production of this technology is supported by sophisticated internal information systems.

Faced with the growing cybersecurity threat, which targets such technologies and the data housed within, the goal of the Philips information security organization is to safeguard enterprise information systems to ensure:

- **Our customer's 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 infrastructure
- **Our compliance to regulations:** Ensure information systems comply or exceed all regulatory requirements

Information security cannot be solved through technology alone. Comprehensive information security requires focus in three domains: People, Processes and Technology (see next page). The Philips Information Security organization implements controls across these three domains to guarantee 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 will continue to focus investments on retaining top-tier cybersecurity talent, enhance cybersecurity tooling and capabilities, and integrate security best practices in everything we do.

Information security focus on people, processes and technology

People

Focuses on the behavioral aspects of employees and improving 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 the process to reduce that risk

Technology

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

6. Privacy

At Philips we have a longstanding commitment to respect the privacy of our customers, consumers and other individuals we deal with, such as patients. Being transparent about how we deal with personal data helps to build trust. As we transform into a digital company, complying with our privacy standards is increasingly important to achieve that commitment.

With our focus on health technology, data privacy and security have become strategically vital, as health data is among the most sensitive types of personal data. Our competitive position relies heavily on the use of this data and public trust is paramount. **Our commitment to privacy goes beyond regulatory compliance**, and we embed privacy and data protection controls throughout the lifecycle of all data.

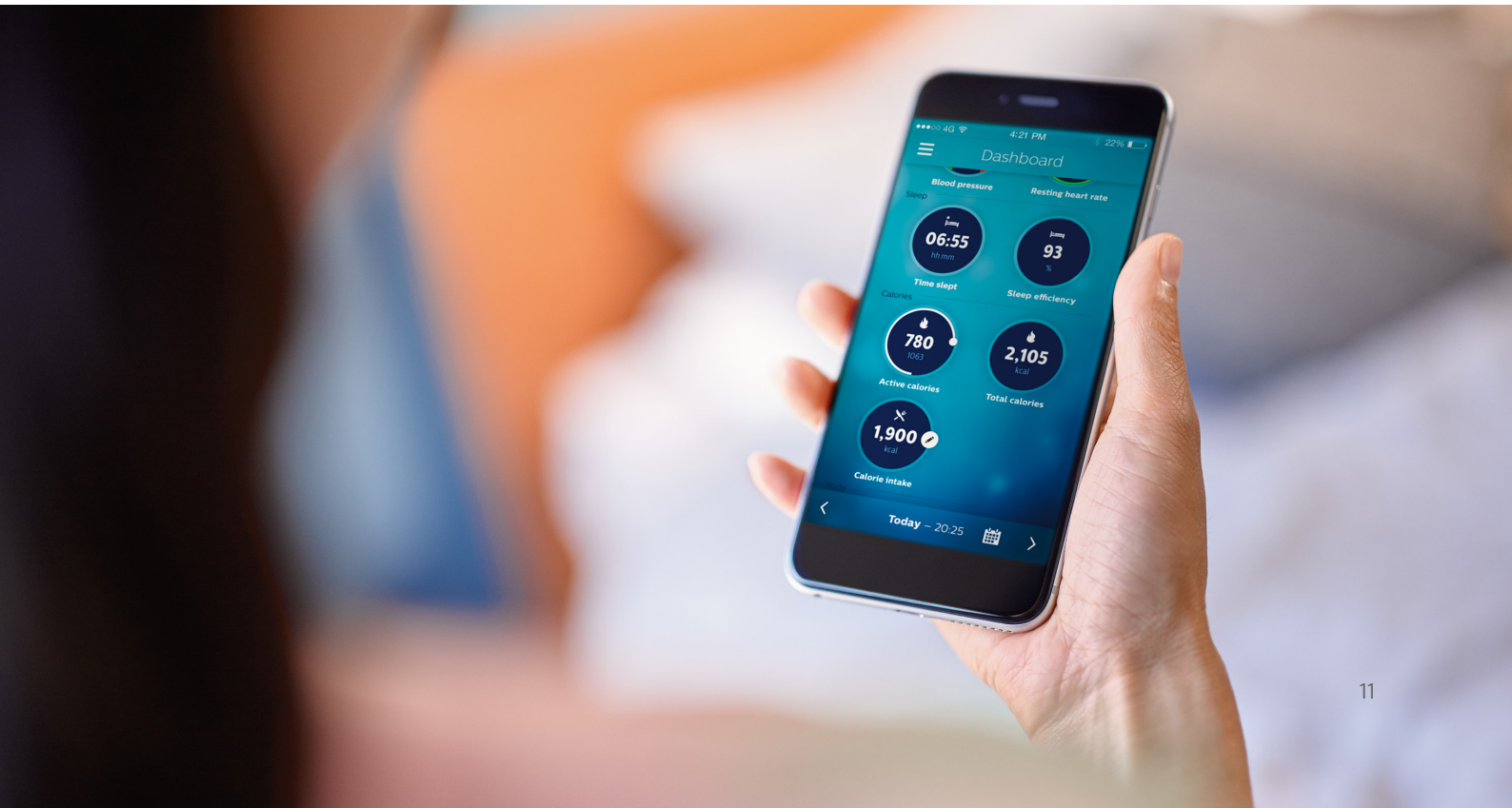
Privacy and data protection are an integral part of our **General Business Principles** whereby we submit ourselves to a number of commitments such as:

- The implementation of Binding Corporate Rules (BCRs) that provide a baseline for privacy protection within Philips worldwide and allow international data transfer between Philips group companies
- Implementation of a privacy program and governance structure which embeds privacy and data protection in the company
- Limiting collection of data, and where appropriate, obtaining consent from individuals
- Notifying individuals as to how collected data will be used, and allowing them to exercise their rights.
- Taking appropriate steps to maintain the accuracy and relevance of the data
- Protecting personal data using appropriate security safeguards

As a global company, Philips needs to take into account all national privacy and data protection laws. Our BCRs and privacy program aim to ensure privacy compliance within Philips worldwide, including where privacy laws are absent.

Philips is committed to high security standards and responsible data stewardship through the principles of **'privacy by design'**. This approach aims to embed privacy and data protection controls throughout the entire data lifecycle, from the early design stage to deployment, collection, use and ultimate data disposition and disposal.

To drive the advances in healthcare made possible by big data, we must foster trust and explain the value to the individual. We need to ensure the fundamental right to privacy, and through our commitment to high security standards and responsible data stewardship we can decrease fear and doubt and offer even greater value to consumers through ongoing innovation.



7. Structures and mechanisms in place

- The **Binding Corporate Rules (BCRs)** are internal rules for processing personal data within Philips, which are also known as the Philips Privacy Rules. The Philips Privacy Rules are largely based on the EU data protection requirements and OECD privacy principles, and prescribe a robust data protection framework within our organization. The Philips Privacy Rules set global data protection requirements that apply to Philips worldwide and enable the international flow of personal data within Philips.

- **Suppliers** that process personal data on behalf of Philips must agree to comply with stringent requirements, as reflected in our BCRs.

- We have dedicated centers of excellence for privacy, product security and information security. The **Philips Global Privacy Office** assists and supports Philips personnel in meeting privacy compliance obligations and establishes the global framework for privacy compliance and risk management.

- **Philips Product Security & Services Office** governs embedding security in product and services during its entire lifecycle, which includes Product Security Risk Assessments, project-independent vulnerability and penetration assessments, specialized product security trainings, and response activities for vulnerabilities identified in existing products and services that are in support.

- We take a holistic, end-to-end approach to product and information security. We have processes and a framework in place to ensure that each step of the product development life cycle is performed to high levels of confidentiality and integrity. As part of our **Secure Product Development Life Cycle** we continuously monitor for vulnerabilities and validate fixes, which activities are supported by our internal Security Center of Excellence.

- We have a **training program for all employees** concerning the safeguarding of personal information and data and the steps that need to be followed to comply with our Philips privacy rules and applicable laws. Employees who handle sensitive data receive additional role based training to further ensure proper data handling. We also have specialized security training programs for our development teams.

- In relation to our **HealthSuite digital platforms**, we contract the hosting of some technical services to third-party Tier 1 providers (such as Amazon, salesforce.com). These providers must certify annually with independent auditors to ISO/IEC 27001 and other relevant security and privacy standards (such as HIPAA/HITECH, SSAE No. 16, NIST SP800-53) where applicable.

8. More information

Philips Product Security Information ›

Philips Privacy Policy web page ›

Appendix:
Product Security Statement

Product Security Statement

This paper summarizes the Philips position on securing our products, services, applications, and systems and describes our processes for providing products with **Security Designed In.**

Background

We at Philips recognize that the security of Philips healthcare, personal health, and home consumer products and services are an important part of your security planning. We are dedicated to helping you maintain the confidentiality, integrity, and availability of personal data, business data and the Philips hardware and software products that create and manage this data.

Threats to the security of devices and personal and healthcare information continue to increase. These threats include malicious security attacks via viruses, worms, and hacker intrusions. Governments around the world have enacted legislation to criminalize many of these cyberattacks and to protect individually identifiable health information (e.g., US-HIPAA, Canada-PIPEDA, general privacy legislation under the European Directive 95/46/EC, Japan-PIPA, and others).

To fulfill our commitment to security, we at Philips maintain a global program to:

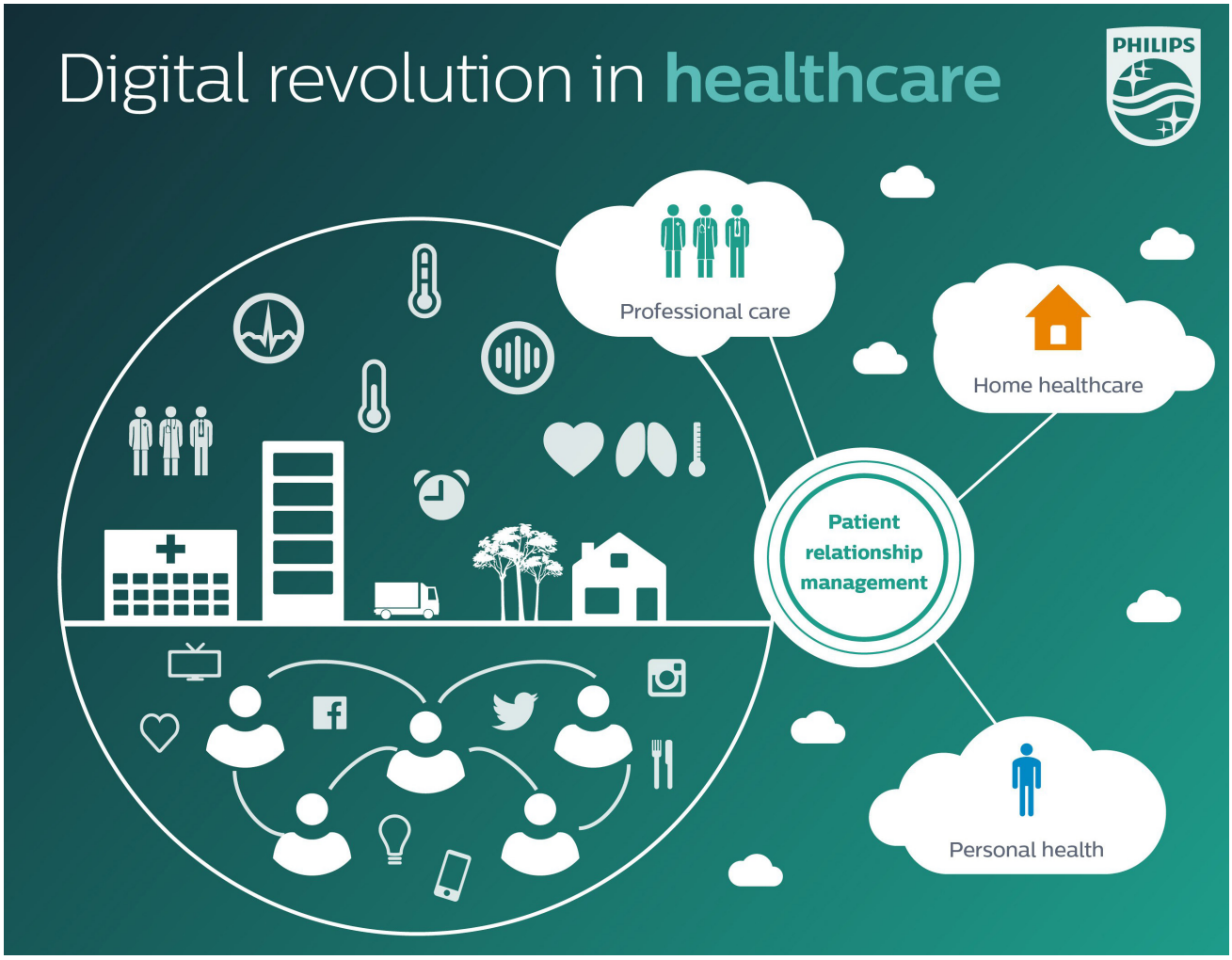
- Develop, deploy, and support advanced security features for our products and services
- Manage security events in the field. Philips participates in industry and government collaborations to help ensure product innovations and clinical information is produced and available at the highest level of quality, availability, and confidentiality.

We implement security within a heavily regulated medical device industry and global climate. Government regulations (e.g., those of the U.S. Food and Drug Administration) require that hardware and software changes be subjected to rigorous verification and validation to assure that high standards of safety and performance are met in all Philips medical devices[1]. Likewise, Philips strives to ensure that same high standard for personal health products, home innovations, and services.

Organization

Philips operates under a global Product Security policy governing design-for-security in product and services creation, as well as risk assessment and incident response activities for vulnerabilities identified in existing products. The Head of Global Product Security oversees the governance and compliance of this policy, reporting directly to the Philips Head of Products and Innovation Excellence. Under direction of the global Product Security Program, Philips has instituted and matured capabilities to include global monitoring, case escalation, rapid response, and full management visibility to security issues.

Table of contents



The Connected/Interconnected Ecosystem

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. This digital 'ecosystem' has helped the industry expand the portfolio of personal and healthcare oriented smart devices, sparked innovation, and increased service efficiency. It has also dramatically escalated the potential of exposure to vulnerabilities and cyberattacks.

Interconnected, interoperable and remotely controlled products and services in our industry are burgeoning. Some areas that present as particularly vulnerable are:

- Provider networks
- Personal health devices
- Remote services
- Sensitive data storage
- Sensitive data on-the-move

The protection of customer networks and private personal/patient data within the ecosystem is of utmost importance. To address this challenge, OEMs such as Philips must take a strategic and integrated view of product security and establish a comprehensive risk-based cybersecurity program.

Internet of Things (IoT)

The 'Internet of Things' (IoT) paradigm envisions the pervasive interconnection and cooperation of smart things over the current and future Internet infrastructure[2]. This revolution in data exchange is empowering people to live healthier lives by using connected devices such as tablets, wearables and hand-held devices to control their own health in a highly personalized manner. For example, Philips in collaboration with partnerships in the industry developed our HealthSuite Digital Platform, which enables IoT devices and applications to operate in conjunction with deep sets of data. HealthSuite Digital Platform offers both a native cloud-based infrastructure and the core services needed to develop and run a new generation of connected, secure healthcare devices and applications.

Analysis of electronic medical records and diagnostic information gathered by imaging equipment, monitors and hand-held personal devices enhance the decision-making powers of professionals and enables a more active role for patients to manage their personal health. These innovations are transforming not just the care of the chronically ill but those who are and want to remain healthy.

Next generation mobile apps, services, and hardware that operate in this rapidly evolving environment will undergo rigorous risk analysis as well as security penetration testing. New devices will be protected with a secure defense framework that identifies users, authorizes consent, and tracks user activity to ensure data privacy.

Key elements of the Philips Product Security Program

In a connected, interoperable healthcare ecosystem the potential for exposure to vulnerabilities and attack is significant. This reality prompts Philips to devote extensive resources to mitigate such threats. Years of work as an industry leader in product security capabilities and product innovation suggest there are five essential components to a successful security program.

1. Governance
2. Testing
3. Coordinated Vulnerability Disclosure
4. Software bill of materials
5. Maturity Roadmap

Governance

Alignment of executive leadership within Philips secures the 'buy-in' necessary to move forward successfully. This in-house team provides continuous oversight, developing strategies and structure to successfully implement the critical attributes of the Product Security Program including policies, risk assessments, security testing, communications, stakeholder requirements, incident management, metrics, and a maturity roadmap for continuous improvement.

The team coordinates the efforts of external players across the cybersecurity ecosystem (customers, vendors, regulators, standards organizations, industry groups and researchers, among others) through ongoing dialogue. This effort is extremely productive in building key relationships and promoting industry best practices toward the safety and security of personal and medical devices. For example, Philips is one of two member medical device manufacturers participating on the U.S. Health and Human Services (HHS) Cybersecurity Taskforce.

Governance of a comprehensive risk management strategy is core to the Philips Product Security Program and mission. That strategy governs a holistic risk management process to prevent, mitigate, and/or remediate pre-market and post-market product security risks, including a focus on three foundational but high impact areas of risk common within the industry, risks that we call the 'Three Deadly Sins':

1. Password Risk
– the risk from a lack of strong password management

2. Encryption Risk
– the risk from a lack of strong data encryption and/or effective data loss prevention solutions

3. Patch Management Risk
– the risk from a lack of effective patch management

Philips emphasizes that consistent adoption of strategies to proactively address the risks of the 'Three Deadly Sins' and other key areas of assessed risk is essential to enable safe and secure products and services and to reduce potential exposures to data breaches, third party vulnerabilities, and sanctions from regulatory institutions and customers.

Testing

A medical devices industry **first**, Philips has established a Security Center of Excellence (SCoE) to develop products which are 'cyber-resilient'. At the SCoE, a dedicated team of ethical hackers, or 'security ninjas', engages in continuous vulnerability and penetration testing to proactively identify product weaknesses. Complementing and strengthening the product security testing of Philips product engineering and development teams, the SCoE testing processes and results are defined in standardized use-case scenarios for a common response approach, which are then leveraged across our entire Philips global enterprise and integrated into risk assessment, secure development lifecycle (SDLC), and maintenance procedures.

Philips product and services security testing covers a wide variety of cybersecurity tasks, including:

- Security vulnerability and penetration testing
- Security risk assessments
- Security source code analysis
- Third party vendor engagements
- US DoD (US Department of Defense) technical product security testing
- Security training tailored to unique roles including product architecture, development, and testing
- Tool validation
- Tool evaluation
- Threat monitoring
- Metrics for product development

Coordinated Vulnerability Disclosure

The development of a coordinated vulnerability disclosure program began with the creation of a Coordinated Vulnerability Disclosure (originally entitled Responsible Disclosure) Policy to reassure customers that proper effort will be made to repair any vulnerabilities and prevent future damage.

Likewise, it is important to handle all security incidents with a sense of urgency and sensitivity. A formal incident response management process has been put into place, which includes documenting all communication, opening a corrective action program, developing a solution, and authoring an incident report.

Confirmed vulnerabilities result in a direct report into government agencies such as the U.S. DHS (ICS-CERT program) and are then communicated through the press to the public. The U.S. FDA pre-and post-market 'Management of Cybersecurity in Medical Devices' guidelines (12/28/16), provide direction on key principals that are globally applicable in practice and in cooperation with other governmental entities and processes. Transparency is key.

Philips was the first major medical device manufacturer to design and implement a Coordinated Vulnerability Disclosure Policy and remains today as a globally recognized industry leader with fully developed and operationally matured processes behind our policy. When public media attention is drawn to security incidents, Philips is often singled out as a manufacturer who's prepared to address difficult issues.

"Philips was the only baby monitor manufacturer praised for responding to **vulnerability warnings**."
– Forbes

"We applaud Philips' commitment to fixing this vulnerability and their established protocol for handling **incoming product** vulnerabilities."
– ARS Technica

"Philips has been **'the most responsive'** of all the companies in addressing the flaw."
– Wall Street Journal

Related: see section for "**Monitoring and Response to Incidents and Vulnerabilities**"

Software Bill of Materials (SBOM)

Companies (Philips included) reliant on integration of third party software open themselves to hidden risks posed by programming code that is not their own.
To prepare for pending legislation on this topic globally, creation of a Software Bill of Materials (SBOM) for every product is essential. This identifies and describes open source and third party software components and allows organizations to quickly respond to possible security vulnerabilities/breaches.

Philips is taking the industry lead to integrate an SBOM into the secure development lifecycle (SDLC) of every Philips product. We will implement processes and procedures to ensure the integrity of any software, firmware, or product developed for our customers.

Related: see section for "Philips open Source Governance and Compliance (SBOM Program)"

Maturity Roadmap

Integrating product security into new product development and consistently deploying product security processes across the portfolio sets the stage for a manageable future. The purpose and intent of a maturity roadmap is to measure and improve Philips' processes and organizational capabilities. Ultimately our desire is to attain improved levels of product security maturity with new product introductions, ongoing service operations, and post-market lifecycle management.

As part of this effort, Philips is focused on a comprehensive product lifecycle management security strategy. It begins with an assessment and monitoring of installed base/legacy products to detect OS obsolescence, incompatibilities, and hardware/firmware vulnerabilities, then allows for ongoing, timely maintenance/updating and lifecycle scheduling.

Philips product security in action

Product Security Assessment/Product Design

Philips proactively conducts internal Product Security assessments to identify potential security weaknesses. Armed with this information, our engineering teams often define configuration changes and re-engineering efforts that will harden the system against outside threats. The same information also drives security design requirements for new products, integrated into Philips secure development lifecycle processes for all products and services. The Philips Product Security Policy requires **Security Designed In** objectives as part of all new product creation efforts.

Monitoring and Response to Incidents and Vulnerabilities

Product engineering groups within Philips monitor new security vulnerabilities on an ongoing basis, including those identified by third party software and operating system vendors and those reported from healthcare enterprises. A global network of Product Security Officers and their teams collect and manage information and address identified vulnerabilities that may affect Philips products and solutions.

When risk events, cyber-security attacks, or incidents are detected or reported, Philips Product Security Incident Response Teams evaluate each real or potential incident with an explicit threat/vulnerability/risk assessment, coordinate a unified response with teams across Philips, communicate status, and follow through to investigate and address security events in accordance with our Product Security policy framework.

Philips Secure Development Lifecycle (SDLC) – Security by Design

Industry trends have shown that cyber-attacks are moving to the application layer of products and pose a significant threat to customers and patient information over the Internet of Things (IoT). According to data collected by the Internet Storm Center, over 70% of attacks on networks are against the application layer. To strengthen the resiliency of our products and services, Philips strengthens our product realization process with capabilities, components, and techniques, including practices that align to ISO standards such as ISO 27034, a practical and well-tested means of incorporating security and privacy within the software development process.

Leveraging this methodology, requirements and controls are addressed at each phase of the secure development lifecycle, including the use of Product Security Risk Assessment (PSRA), Privacy Assessment (PIA) processes, static code analysis, third party Software Bill of Materials (SBOM) analysis, ethical penetration testing, and continuous product security training across the Philips organization. While tools and processes are key to the Philips SDLC, Security by Design is a mindset that requires an end-to-end approach that begins with architecture and high-level design which progresses through to coding, testing, and post-market support.

Philips Open Source Governance and Compliance Program (Governance of SBOM)

Most software built today incorporates open source and other commercial off-the-shelf components. These third party components may introduce vulnerabilities into a product to which the manufacturer is unaware. A 'software bill of materials' (SBOM) carefully documents the tools used to build an application and identifies exactly what third party components are included. This helps security organizations respond quickly and precisely to potential risks.

Many manufacturers do not have an accurate bill of material listing for each of their products. With no accurate listing, they do not have a good understanding of the vulnerabilities associated with the product components. Without SBOM product information, and faced with a vulnerability issue, there is no easy way to identify the affected code and introduce a solution. Hence, an agile response is exceedingly difficult.

Pending U.S. legislation seeks to assure the security of product software. The Cyber Supply Chain Management and Transparency Act requires government agencies to obtain software BOMs for any new products they purchase. It will also require obtaining SBOMs for "any software, firmware, or products containing a third party or open source binary component[1]."

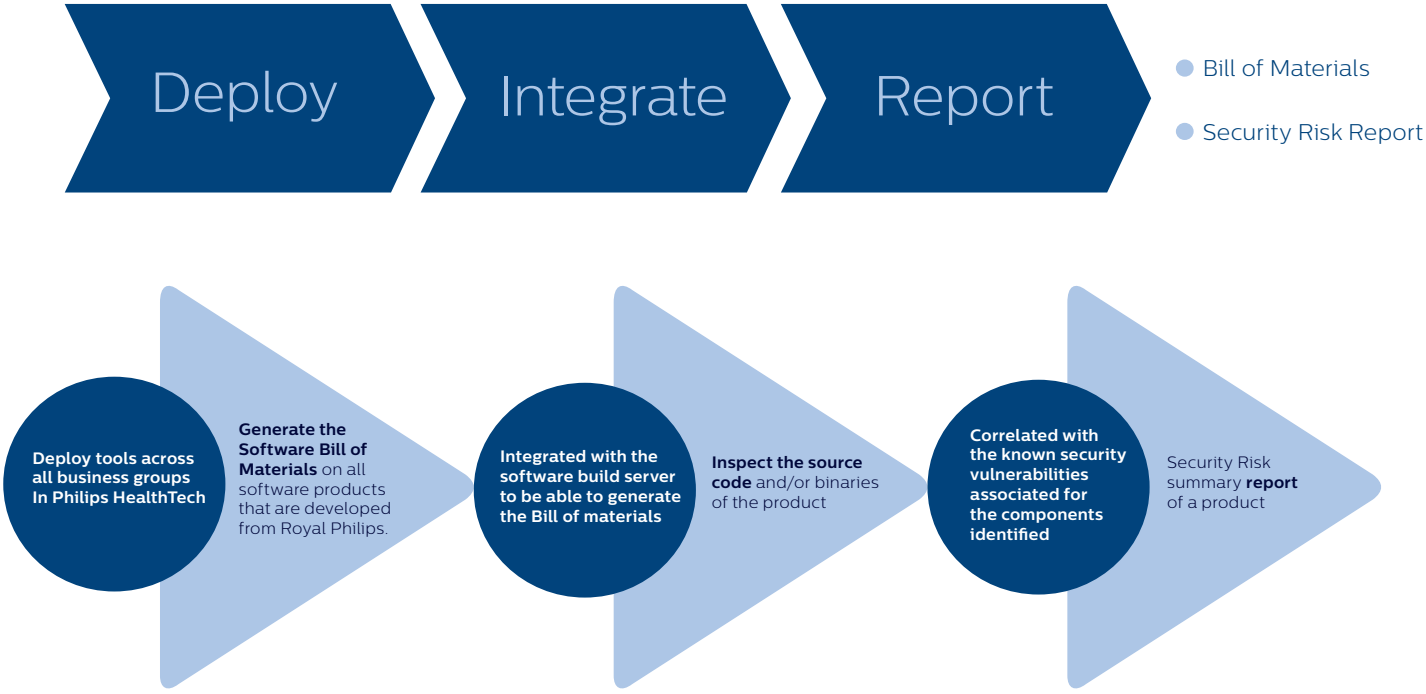
As a result of this pending legislation, requirements are being adopted for the governance and disclosure of security vulnerabilities or defects for open source and third party software, such as those adopted by the U.S. Veterans Administration and defined in the U.S. National Institute of Standards and Technology 800-53 (NIST 800-53).

NIST 800-53 is a U.S. publication that recommends security controls for federal information systems and organizations and documents security controls for all U.S. federal information systems, except those designed for national security[2].

Philips is out in front of these requirements with our SBOM governance program which includes the following three phases:

- **Deploy** – Generate the Software Bill of Materials on all software driven products that are developed by Philips. This is being accomplished by deploying SBOM tools across all business groups.
- **Integrate** – Integrate SBOM tooling and processes into the software development/build process. Inspect the source code and/or binaries of each product.
- **Report** – Create a Security Risk summary of each product. Then correlate that summary with the known security vulnerabilities associated with identified components.

Approach to Open Source Governance and Compliance



Identifying and describing open source and third party software components within a product portfolio allows for quick response to possible security vulnerabilities/breaches. Following are seven key elements associated with a successful SBOM program:

1. Document SBOM requirements
2. Integrate SBOM into the software development lifecycle process, including updating and maintenance
3. Identify SBOM vulnerabilities and license issues and incorporate findings into security risk assessments, and remediate as per the risks assessed
4. Include SBOM in all relevant product documentation
5. Monitor SBOM continuously for new vulnerabilities and security software updates
6. Update SBOM in relevant product documents and security risk assessments
7. Adjust overarching SBOM requirement as necessary based on changes in government regulation

The Philips Product Security SBOM process will be integrated into the system development life cycle for each of our products in accordance with the Philips Product Security policy. New systems will meet these expectations and be prepared for future upgrades. Legacy systems with security issues will be addressed with upgrades, network mitigations, or replacement.

Operating Systems and Patch Management

Some Philips products use third party commercial computer Operating Systems (OS) like Microsoft Windows. We continuously monitor relevant vendor and industry/media security announcements and perform risk assessments on current medical devices that are affected by newly discovered vulnerabilities.

Microsoft releases information on MS Windows security patches (hotfixes) on a regular basis. Impact assessments of these hotfixes by Philips' product engineering teams typically begin within 48 hours of Philips' awareness of a new security vulnerability or patch availability. Following assessment, an indication of Philips' response for affected products is available to users typically within 5 to 12 business days for most products.

Depending on the nature of the threat and the affected product in question, a validated "fix" or software update may be released. If the recommended response requires a change to the system software of a medical device, a software update may be released. Information concerning the availability and applicability of such updates is likewise available via Philips' standard service channels and, for some products, can be found via our website.

In an effort to provide you with this important information in a timely and convenient manner, the Philips Product Security website features access to dynamic product-specific vulnerability information. This information is formatted into simple, product-specific tables listing known software vulnerabilities and their current status, recommended customer action and general comments. Please visit the Philips Product Security website to access this information. If you have any questions regarding the vulnerability tables, patch management, or other product security interests, contact Philips by email productsecurity@philips.com or directly contact your Philips Field Service Engineer.

Malware Protection

To deploy and maintain effective operation of your equipment, Philips products are delivered to operate within compliance of specific system and security specifications. These product specifications may include device configuration, network, operating system, and/or software requirements for malware protection. Please refer to your specific product documentation or instructions for use for more information.

Philips Product Security Website

Philips provides a variety of information resources on our Product Security website, including, Security Bulletins, FAQs, vulnerability information, links to industry resources, product security white papers, and other Product Security highlights.

Medical Device MDS² Forms

To assist our U.S. customers in meeting their HIPAA obligations under the 2005 Security Rule, Philips has taken the lead in publishing Product Security information[3]. Philips has taken many steps to enhance the security of our medical devices in response to customer requests. When used properly, the security features of Philips healthcare products make it easier for users to meet their obligations to ensure the confidentiality, integrity, and availability of patients' health information. In light of the increased focus on medical device security and compliance with the HIPAA Security Rule in the US, the Healthcare Information and Management Systems Society (HIMSS) created a standard "Manufacturer Disclosure Statement for Medical Device Security" (MDS²). The MDS² is intended to supply healthcare providers with important information that can assist them in assessing and managing the vulnerabilities and risks associated with electronic Protected Health Information (ePHI) created, transmitted, or maintained by medical devices.

Philips MDS² forms are available to customers via our Product Security website at: www.philips.com/productsecurity.

Customer Role in Product Security Partnership

We recognize that the security of Philips products needs to be an important part of your security-in-depth strategy. However, protection can only be realized if you implement a comprehensive, multi-layered strategy (including policies, processes, and technologies) to protect information and systems from internal and external threats. Following industry-standard practice, your strategy should address physical security, operational security, procedural security, risk management, security policies, and contingency planning. The practical implementation of technical security elements varies by site and may employ a number of technologies, configurations, and software solutions. As with any computer-based system, protection can include firewalls, network segmentation, and/or other security devices between the medical system and your institution's network. Such perimeter and network defenses are essential elements in a comprehensive medical device security strategy.
Any device connection to an internal or external network should be done with appropriate risk management for product effectiveness and data and systems security.

Policies on Third-Party Software and Patching

Philips sells highly complex medical and personal devices and systems. Only Philips-authorized changes are to be made to these systems, either by Philips personnel or under Philips explicit published direction. With the current rise in security threats, Philips product engineering groups work to qualify security-related third party software and solutions for selected equipment. Moreover, we continue to treat patient and operator safety as our primary concern, and we are required to follow regulatory and quality assurance procedures to verify and validate modifications to our medical devices. As with other medical devices, any "software only" Philips products should be used only on computers and networks that are properly secured in accordance with your Philips product documentation, service agreements, and instructions for use. We strongly suggest that your security staff monitor system and application vulnerabilities and keep the operating system and other installed software running on your system patched and up-to-date.

Philips sells a broad range of devices, from consumer lifestyle products and home monitoring systems to image acquisition and viewing systems, IT-oriented PACS to 24/7 life-critical systems, and real-time patient monitors. The diverse nature of our product portfolio has led us to support a wide range of solutions including installation and maintenance of third party software on our systems. Please contact Philips for more specific information on your particular product[4].

General Case

Most Philips equipment does not permit third party software installation of any kind by the customer (e.g., anti-virus scanners, office productivity tools, system patches, on-platform firewalls, etc.) unless documented by Philips as an operating specification requirement or prior written consent is attained. Unauthorized modifications to Philips products could void your warranty and alter the regulatory status of the device. Any resulting service required from unauthorized modification is not covered under our service agreements. Such unauthorized modifications can affect the performance or safety of your device in unpredictable ways. Philips is not responsible for equipment that has been subject to unauthorized modification.

When Philips authorizes the use of third party software, system patches, or upgrades, the authorized installation is typically carried out by (1) Philips at the time of manufacture or installation or, (2) a post-installation Philips-qualified Service Engineer.

Exceptions

Philips may permit in certain circumstances the installation or enabling of third party software directly by a Philips-qualified Service Engineer, but always under explicit published guidance of Philips and only to be applied to the particular system and version covered by the Philips written authorization.

Prior to considering the install or enablement of any third party software on a Philips product, you should contact your local Philips service representative to determine if your particular product has been qualified for that specific software and, if so, what restrictions may apply.

It is important to understand that any unauthorized modification of a Philips medical device or system (e.g., product firewall changes, software patches, security software, utilities, games, music files, other software programs, etc.) can adversely affect system performance or safety in unpredictable ways, thereby depriving your staff and their patients of protections afforded by Philips, regulatory, and quality requirements. Possible detrimental side effects of these installations or modifications might include:

1. Opening or widening of pathways which could allow a compromise of access or control
2. Introduction of viruses, spyware, Trojans, backdoor access, or other remote agents
3. Installation of unauthorized updates that could lead to product and system vulnerabilities

Should you suspect or know of any unauthorized modifications to your Philips product or solution, you should immediately report it to Philips Customer Services or your Field Service Engineer who will assist you in determining the appropriate action.

Philips Remote Service

Philips has created a global, web-based Philips Remote Services network (RSN) for connecting many of your Philips systems to our advanced service resources. This state-of-the-art design provides your equipment with a single point-of-network access to on-site Philips equipment using Virtual Private Network technologies. This secure tunnel approach was developed to provide a best-in-class remote service solution that secures the connection through explicit authorization and authentication control with encryption of all of the information in the service session.

Philips Product Innovations and Solutions in a Changing World

In line with the need to increase security of our products, Philips continues to examine and re-engineer existing products to best accommodate the requirements of our security-minded customers. We are deeply engaged in creating the products of tomorrow based on fundamental security principles.

We will continue to work closely with providers, IT organizations, and consumers to provide flexible solutions to today's problems even as we create new Security Designed In products. Questions about our efforts to improve the security of our products can be directed to your field service or sales representative or productsecurity@philips.com. If your concern extends to how Philips manages personal data (i.e., privacy), you can email your questions to healthcare.privacy@philips.com.

Thank you for your continued interest in the many innovative solutions provided by Philips.

1 U.S. FDA's Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software. http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077812.html

2 Privacy in the Internet of things: Threats and Challenges, https://arxiv.org/abs/1505.07683

3 To obtain copies of the Manufacturer Disclosure Statement for Medical Device Security (in HIMSS MDS2 standard form) for Philips' products, visit http://www.healthcare.philips.com/main/support/productsecurity/mds2.wpd

4 Philips Support contact information:
Philips Health Care:
- North America – 1 800 669 1328 (or +1 321 253 5693)
- Asia – +85 2 2821 5888
- Europe, Middle East, Africa – +49 7031 463 2254
- Latin America – +55 11 2125 0744
- Canada – 1 800 291 6743

Global Contacts (Health Care, Personal Health, Consumer Products)
- http://www.philips.com/c-cs/global-country-selector.html
- Select country, choose "Support", and select "Contact"

5 Application of Risk Management to IT-networks Incorporating Medical Devices, http://www.iso.org

6 U.S. Department of Veterans Affairs Medical Device Isolation Architecture Guide, v2.0, available at the HIMSS website http://www.himss.org/ASP/topics_FocusDynamic.asp?faid=101

7 Healthcare Information and Management Systems Society (HIMSS) Medical Device Security Workgroup http://www.himss.org/ See Topics an Tools > Medical Device Security

8 U.S. FDA Postmarket Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff (Dec. 2016), http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm482022.pdf

9 IHE is a joint initiative of the Healthcare Information and Management Systems Society (HIMSS) and the Radiological Society of North America (RSNA) http://www.ihe.net/

www.philips.com/productsecurity

www.philips.com