Product Security Statement

Philips

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

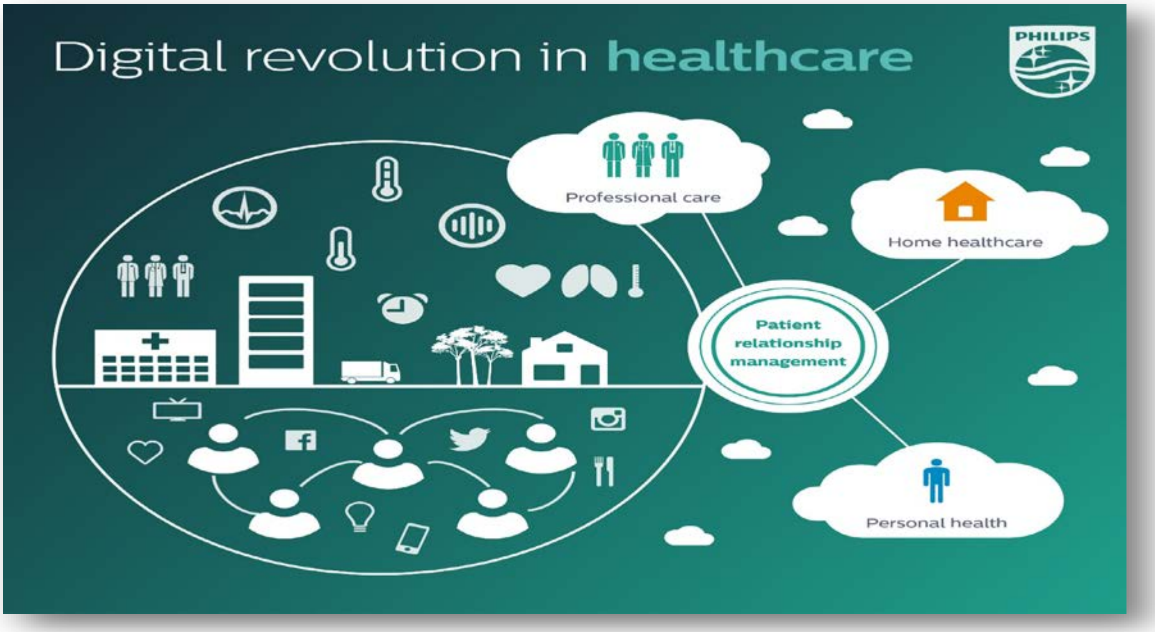
Philips operates under a global Product Security policy governing design-for-security in product and services creation, as well as risk assessment and incident response activities for vulnerabilities identified in existing products. The Head of Global Product Security oversees the governance and compliance 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.

PHILIPS

sense and simplicity

TABLE OF CONTENTS

Digital Revolution


Digital revolution in healthcare
PHILIPS
Professional care
Home healthcare
Patient relationship management
Personal health

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.

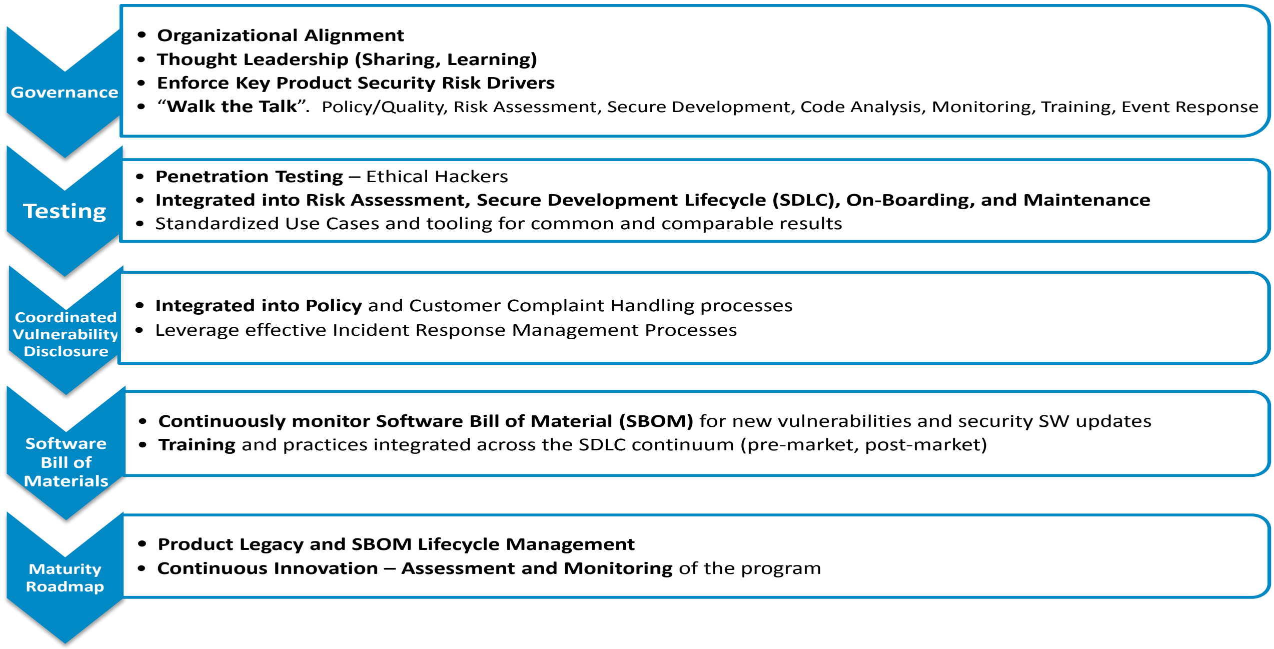
Analysis of electronic medical records and diagnostic information gathered by imaging equipment, monitors and hand-held personal devices enhance the decision-making powers of professionals and enables a more active role for patients to manage their personal health. These innovations are transforming 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

- **Organizational Alignment**
- **Thought Leadership (Sharing, Learning)**
- **Enforce Key Product Security Risk Drivers**
- **"Walk the Talk"**. Policy/Quality, Risk Assessment, Secure Development, Code Analysis, Monitoring, Training, Event Response

Testing

- **Penetration Testing** – Ethical Hackers
- **Integrated into Risk Assessment, Secure Development Lifecycle (SDLC), On-Boarding, and Maintenance**
- Standardized Use Cases and tooling for common and comparable results

Coordinated Vulnerability Disclosure

- **Integrated into Policy** and Customer Complaint Handling processes
- Leverage effective Incident Response Management Processes

Software Bill of Materials

- **Continuously monitor Software Bill of Material (SBOM)** for new vulnerabilities and security SW updates
- **Training** and practices integrated across the SDLC continuum (pre-market, post-market)

Maturity Roadmap

- **Product Legacy and SBOM Lifecycle Management**
- **Continuous Innovation – Assessment and Monitoring** of the program

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 at 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 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.

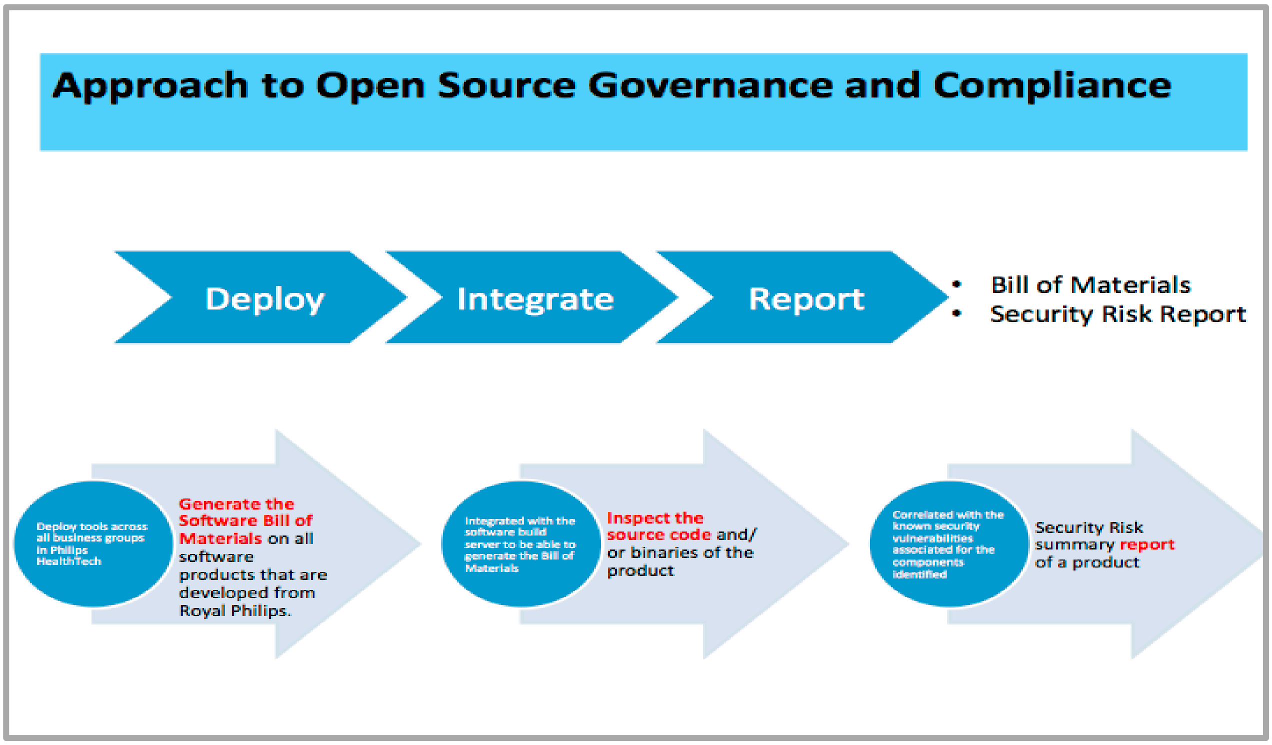
Pending U.S. legislation seeks to assure the security of product software. When passed, The Cyber Supply Chain Management and Transparency Act will require government agencies to obtain software BOMs for any new products they purchase. It will also require obtaining SBOMs for "any software, firmware, 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

Deploy

Integrate

Report

- Bill of Materials
- Security Risk Report

Deploy tools across all business groups in Philips HealthTech

Generate the Software Bill of Materials on all software products that are developed from Royal Philips.

Integrated with the software build server to be able to generate the Bill of Materials

Inspect the source code and/ or binaries of the product

Correlated with the known security vulnerabilities associated for the components identified

Security Risk summary **report** of a product

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 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 MDS^2 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” (MDS^2). The MDS^2 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 MDS^2 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 both 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.htm*

[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 and 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/*.

PHILIPS

Philips reserves the right to make changes in specifications and/ or to discontinue any product at any time without notice or obligation and will not be liable for any consequences resulting from the use of this publication.

Philips Electronics
www.philips.com/productsecurity