Product Security Policy Statement

Philips Healthcare

This summarizes Philips Healthcare position on securing its medical products and systems in your healthcare enterprise and describes our processes for providing products with *Security Designed In*.

Background

We at Philips Healthcare recognize that the security of Philips Healthcare products and services is an important part of your organizational security planning. We are dedicated to helping you maintain the confidentiality, integrity, and availability of both electronic personal data (e.g., Protected Health Information – ePHI) and the Philips hardware and software products that create and manage these data.

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

To fulfill its commitment to security, Philips Healthcare maintains a global program to (a) develop and deploy advanced security features for our products and services and (b) manage security events in the field. At the medical device industry level, Philips works on the HIMSS Medical Device Security Workgroup[1] and strives to ensure that new customer security options are included in industry standards such as the Integrated Healthcare Enterprise[2]. We also work to continuously improve our own internal Information Technology Enterprise security, including continuous security improvement in both the product development and service delivery environments.

Philips Healthcare implements security within a heavily regulated medical device industry. Government regulations (e.g., those of the US 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 of Philips medical devices[3].

Philips Healthcare Product Security Activities

Organization

Philips Healthcare operates under a global Product Security policy governing design-for-security in product creation, as well as risk assessment and incident response activities for vulnerabilities identified in existing products. The Director of Product Security oversees the implementation of this policy, reporting directly to the Philips Healthcare Chief Technology Officer. Philips Healthcare has instituted a global problem-tracking and escalation system that provides rapid response with full management visibility to security issues.

PHILIPS

sense and simplicity

Monitoring and Response to Vulnerabilities

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

Philips Product Security Incident Response Teams evaluate each real or potential breach with an explicit threat/vulnerability/risk assessment and develop vulnerability response plans as necessary. We want to inform you, our customers, of vulnerabilities that impact your systems, and proceed with mitigation development and deployment while keeping you well informed.

Operating System Patch Management

Some Philips Healthcare products use non-Philips commercial software and/or commercial computer Operating Systems (OS) like Microsoft Windows. Philips continuously monitors relevant vendor and industry/media security announcements and performs risk assessments on current medical devices that are most 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 the Philips Healthcare website.

In an effort to provide you with this important information in a timely and convenient manner, Philips Product Security website now 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 Healthcare Product Security website to access this information. If you have any questions regarding the OS vulnerability tables or patch management, contact Philips Healthcare by email *productsecurity@philips.com* or directly contact your Philips Field Service Engineer.

Malware Protection

Philips products that support additional malware protection are either delivered with pre-installed anti-virus software or you, the customer, are advised on the installation of permissible, Philips-validated, anti-virus software.

In many of our products, we provide you with a controlled update repository to reduce the risk of equipment outage due to unauthorized or faulty anti-virus signature updates. If available, this service is included in our remote services agreement.

Even when our product is delivered to you with anti-virus software or when you, the customer, install permissible, Philips-validated, anti-virus software, the anti-virus software must be configured according to the Philips-provided guidance. This guidance includes the permissible sources for signature updates in order to maintain safe and effective operation of your equipment. When Philips has validated anti-virus software for your product, it remains your organization's responsibility to regularly check and, if needed, follow the Philips-prescribed update process for the anti-virus software. All changes to your medical device or system should be authorized by Philips documentation or in writing from Philips.

Product Assessment/Product Design

Philips Healthcare 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. The Philips Product Security Policy requires *Security Designed In* objectives as part of all new product creation efforts.

Philips Product Security Website

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

MDS² Forms

To assist our USA customers in meeting their HIPAA obligations under the 2005 Security Rule, Philips Healthcare has taken the lead in publishing Product Security information[4]. 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 USA, 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 Healthcare products is an important part of your facility's 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 external and internal 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, including firewalls, virus-scanning software, authentication technologies, etc. As with any computer-based system, protection must be provided such that firewalls and/or other security devices are in place between the medical system and any externally accessible systems. The USA Veterans Administration has developed a widely used Medical Device Isolation Architecture for this purpose[5]. Such perimeter and network defenses are essential elements in a comprehensive medical device security strategy. Any connection of a device to a hospital network should be done with appropriate risk management for safety, effectiveness, and data and systems security. For guidance on risk management, see the IEC-80001-1 standard[6].

Policies on Third-Party Software and Patching

Philips Healthcare sells highly complex medical 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 are working to qualify security-related third-party software on selected equipment. However, we continue to treat patient and operator safety as our primary concern, and we are required to follow government-regulated quality assurance procedures to verify and validate modifications to the operation of our medical devices. As with other medical devices, any "software only" Philips products should be used only on properly secured computers and networks. 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 up-to-date.

Philips Healthcare sells a broad range of devices, from image acquisition and viewing systems and IT-oriented PACS to 24/7 life-critical, real-time patient monitors. The diverse nature of our products has led us to support different means of installation and maintenance for third-party software on our systems. Please contact Philips Customer Services for more specific information on your particular product.

General Case

Most of Philips Healthcare 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.) without prior written consent. Unauthorized modifications to Philips Healthcare products could void your warranty and alter the regulatory status of the device. Any resulting service required is not covered under our service agreements. Such modifications can affect the performance or safety of your device in unpredictable ways, and Philips is not responsible for equipment that has been modified.

When Philips authorizes the use of anti-virus scanners, system patches, or upgrades, the scanner/patch/upgrade installation is typically carried out by (1) Philips Healthcare at the time of manufacture or installation or, (2) post-installation by a Philips-qualified Service Engineer.

Exceptions

In very few of our systems, Philips does permit the installation or enabling of third-party software directly by your designated Philips system administrator, but always under explicit published guidance of Philips Healthcare and only to be applied to the particular system and version covered by the Philips written documentation.

Prior to installing or enabling any third-party software on a Philips Healthcare 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. The qualification and use of these software products vary by Philips product.

It is important to understand that any unauthorized modification of a Philips medical device or system (e.g., in-product firewall change or installation of patches, virus-detection software, utilities, games, music files, updates, etc.) can adversely affect system performance or safety in unpredictable ways, thereby depriving your staff and their patients of protections afforded by government regulatory requirements for medical devices as well as Philips extensive quality system for the development, manufacturing, and testing of its devices. Possible detrimental side effects of these installations or modifications might include:

1. the opening or widening of pathways which could allow a compromise of access or control
2. the invisible introduction of viruses, spyware, trojans, backdoor access, or other remote agents
3. the installation of an unauthorized update that converts a stable system component into one with a vulnerability

Should you suspect or know of any unauthorized modifications to your Philips medical device or system, you should immediately report it to your Philips Field Service Engineer who will assist you in determining the appropriate corrective action to bring your device or system back into specification.

Philips Remote Service

Philips Healthcare has created a global, web-based Philips Remote Services network (PRS) 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 Healthcare in a Changing World

In line with the need to increase security of our medical products, Philips Healthcare 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 your care providers and your IT organizations to provide flexible solutions to today's problems even as we create new *Security Designed In* medical 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 beyond product and service security to how Philips Healthcare 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 healthcare solutions provided by Philips Healthcare.

[1] Healthcare Information and Management Systems Society (HIMSS) Medical Device Security Workgroup *http://www.himss.org/* see Topics and Tools >> Medical Device Security.

[2] 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/*.

[3] For more information, see the U.S. Food and Drug Administration Information for Healthcare Organizations about FDA's Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software at *http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077812.htm*

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

[5] See USA 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*

[6] Application of Risk Management to IT-networks Incorporating Medical Devices, *http://www.iso.org*

Philips Healthcare is part of Royal Philips Electronics

www.philips.com/productsecurity
healthcare@philips.com

Printed in the USA
4522 962 69671 * AUG 2011