

# Product Security Policy Statement

## Philips Medical Systems

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

### Background

Philips Medical Systems is dedicated to helping you maintain the confidentiality, integrity, and availability of both electronic Protected Health Information (ePHI) and the hardware and software products that create and manage these data.

Over the last few years, threats to the security of devices and healthcare information have increased dramatically. 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., HIPAA in the USA, BC 73, general privacy legislation under the European Directive 95/46/EC, Japan HPB517, and others).

To fulfill its commitment to security, Philips Medical Systems 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<sup>1</sup> and strives to ensure that new customer security options are included in industry standards such as the Integrated Healthcare Enterprise.<sup>2</sup> 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 Medical Systems 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.<sup>3</sup>

### Philips Medical Systems Product Security Activities Organization

Philips Medical Systems 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 Medical Systems Chief Technology Officer. Philips Medical Systems has instituted a global problem-tracking and escalation system that provides rapid response with full management visibility to security issues.

### Monitoring and Response to Vulnerabilities

Product engineering groups within Philips Medical Systems 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 Medical Systems products and solutions.

The Philips logo, consisting of the word "PHILIPS" in a bold, blue, sans-serif font.

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 Medical Systems 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 3 to 5 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 on the Philips Medical Systems “vulnerability table” 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, tips, and general comments.

Please visit the Philips Medical Systems Product Security website to access this information:  
<http://www.medical.philips.com/main/productsecurity/vulnerabilities/>

If you have any questions regarding the patch management or OS vulnerability tables, contact Philips Medical Systems by email [productsecurity@philips.com](mailto:productsecurity@philips.com) or directly contact your Philips Field Service Engineer.

#### Product Assessments/Product Design

Philips Medical Systems 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 Medical Systems now 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.

#### MDS<sup>2</sup> Forms

To assist our USA customers in meeting their HIPAA obligations under the 2005 Security Rule, Philips Medical Systems has taken the lead in publishing Product Security information.<sup>4</sup> 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 Medical Systems 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 Health Information and Management Systems Society (HIMSS) has created a standard “**Manufacturer Disclosure Statement for Medical Device Security**” (MDS<sup>2</sup>). The MDS<sup>2</sup> 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<sup>2</sup> forms are available to customers on our Product Security website at:  
<http://www.medical.philips.com/main/productsecurity/mds2/>

## Customer Role in the Product Security Partnership

We recognize that the security of Philips Medical Systems products is an important part of your facility's security-in-depth strategy. However, these benefits 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.<sup>5</sup> Such perimeter and network defenses are essential elements in a comprehensive medical device security strategy.

### Policies on Third-Party Software and Patching

Philips Medical Systems 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.

Philips Medical Systems sells a broad range of devices, from image acquisition and viewing systems and IT-oriented PACS to 24x7 life-critical real-time monitors. The diverse nature of our products has led us to support two means of installation and maintenance for third-party software on our devices. Please contact Philips Customer Services for more specific information on your particular product.

### General Case

Most of Philips Medical Systems equipment does not permit third-party software installation of any kind by the customer (e.g., virus-scanners, office productivity tools, system patches, on-platform firewalls, etc.) without prior written consent. Unauthorized modifications to Philips Medical Systems products void our warranty. 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 virus-scanners, system patches, or upgrades, the scanner/patch/upgrade installation is carried out by either Philips Medical Systems at the time of manufacture or 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 Medical Systems and only to be applied to the particular system and version covered by the Philips written documentation.

In the case where the installation of virus-scanning software is permitted on a particular piece of equipment, your system administrator is responsible for updating the virus definition files as necessary.

Prior to installing or enabling any third-party software on a Philips Medical Systems 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 that you, as a valued healthcare customer, 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,

