Shared Roles for System and Data Security

English

Lumify Ultrasound System

PHILIPS

Contents

4535 619 41961_A/795 * FEB 2018

Philips

Contents

4535 619 41961_A/795 * FEB 2018

Philips

1 Introduction

This document discusses security on the Lumify Ultrasound System. Philips provides different configuration options for the Lumify Ultrasound System, including Bring Your Own Device (BYOD). Whereas other Philips ultrasound systems are delivered as complete systems, with restrictions on what is authorized and available for the system, Lumify host devices can be acquired, configured, and maintained by the healthcare organization or by individuals.

Eligible customers may select a bundled version of the product, which is sold as a complete system (both hardware and software). In both the BYOD and bundled versions, the device must be configured and maintained by the healthcare organization or individual.

These guidelines are designed to help healthcare organizations understand how the security of the Philips Lumify app and patient data can be compromised, and to highlight Philips efforts to ensure that safeguards are in place to help prevent security breaches.

For ultrasound-system security resources, such as security bulletins, FAQs, and vulnerability information, see the Philips Product Security website:

www.philips.com/productsecurity

For information about the Lumify Ultrasound System, visit the Lumify portal:

www.philips.com/lumify

4535 619 41961_A/795 * FEB 2018

Philips has taken care to ensure the accuracy of this document. However, Philips assumes no liability for errors or omissions and reserves the right to make changes without further notice to any products herein to improve reliability, function, or design. Philips may make improvements or changes in the products or programs described in this document at any time.

Philips makes no representation or warranty to the user or any other party with respect to the adequacy of this document for any particular purpose or with respect to its adequacy to produce a particular result. The user's right to recover damages caused by fault or negligence on the part of Philips shall be limited to the amount paid by the user to Philips for the provision of this document. In no event shall Philips be liable for special, collateral, incidental, direct, indirect or consequential damage, losses, costs, charges, claims, demands, or claims for lost profits, data, fees, or expenses of any nature or kind.

Unauthorized copying of this document, in addition to infringing copyright, might reduce the ability of Philips to provide accurate and current information to users.

Non-Philips product names may be trademarks of their respective owners.

General Information

The following general information applies to the security of Philips ultrasound software and patient data.

- Philips ultrasound systems do not support multiple-user-session operations. They are designed as single-user devices. Clinical-use access over a network is unsupported.
- Ultrasound systems are not long-term storage devices. Persistent patient data must be archived to a DICOM PACS, to a network share, or to a local directory.

4535 619 41961_A/795 * FEB 2018

Philips

2 Control of Security Vulnerabilities on Philips Products

Philips is dedicated to helping all customers maintain the confidentiality, integrity, and availability of patient data while ensuring that their ultrasound systems continue to generate and manage this information with complete security. Ultrasound systems may become vulnerable to security breaches when they are connected to a network.

Strategy for Defense-in-Depth Security

Within the healthcare organization, maintaining the security of patient data and Philips products requires a defense-in-depth security strategy, one that is comprehensive and multilayered (including policies, processes, and technologies) for protecting information and systems from internal and external threats.

For specific information about security within your organization, consult with the security specialists in the following offices or those with similar responsibilities:

- Chief information security officer
- Chief information officer
- HIPAA privacy or security officer (in the United States)
- Safety officer

To learn about general security issues or specific vulnerabilities of your ultrasound system, contact your Philips representative.

4535 619 41961_A/795 * FEB 2018

Philips

Regulatory Environment

The development and manufacture of medical devices is tightly regulated, as is the security and privacy of patient information held by healthcare providers. This creates challenges for both healthcare providers and manufacturers in responding quickly to new threats to the security of patient data stored on medical devices.

Protection of Electronic Patient Health Information

One of the most important assets to protect with security measures is patient health information. As an example, the following regulations require patient health information to remain confidential, and they specify security measures to guard patient information:

- Health Insurance Portability and Accountability Act (HIPAA), United States of America (www.hhs.gov/ocr/privacy/)
- European Medical Device Directive 93/42/EEC
- Japan's HPB517
- HIPAA-related portions of the U.S. federal economic-stimulus act (or HITECH), formally known as the American Recovery and Reinvestment Act of 2009

Role of Philips in the Product Security Partnership

Philips operates under a global Product Security Policy that governs design-for-security in product creation, risk assessment, and incident-response activities for vulnerabilities identified in existing products. Philips has instituted a global problem-tracking and escalation process that provides visibility to security issues involving Philips systems.

Response to Vulnerabilities

Product engineering groups within Philips monitor continuously for new security vulnerabilities of our systems, including those identified by third-party-software and operating-system vendors and those reported from individual healthcare organizations.

4535 619 41961_A/795 * FEB 2018

Philips

A global network of response teams dedicated to product-security incidents collects and manages information and addresses the vulnerabilities that affect Philips products and solutions. The response teams continue to expand their activities toward global coverage of all systems.

The goal is for the appropriate response team to evaluate each real and potential breach of security with an explicit assessment of the risk, threat, or vulnerability and to develop, as required, a vulnerability response plan that includes qualification and communication procedures. This means that Philips intends to simultaneously inform customers of system vulnerabilities while proceeding with development and deployment of risk-mitigation efforts. For more information about system vulnerabilities, see this website:

www.philips.com/productsecurity

Design Improvements

Philips actively conducts internal product security assessments to identify potential security weaknesses. With that information, Philips engineering teams often define configuration changes and re-engineering efforts that harden the system against outside threats. The same information also drives security design requirements for new products. The Philips Product Security Policy requires design-for-security objectives as part of all new product-creation efforts.

Role of Customers in the Product Security Partnership

WARNING

Unauthorized modifications to your Android device ("rooting" or "jailbreaking") can cause the ultrasound system to malfunction, which may lead to misdiagnosis.

4535 619 41961_A/795 * FEB 2018

Philips

CAUTION

Android devices have many applications available for installation through the Google Play store. However, to minimize the risk to patient data security, Philips recommends that you install applications only from trusted sources and that you limit their use to business needs.

It is your responsibility to ensure the security of your device and of patient data to meet your local security policies and regulatory requirements. Consult your Healthcare IT Security department to ensure that the security profile of your device is configured in accordance with your specific requirements for information security.

The practical implementation of technical security elements varies by site and may employ a number of technologies, including firewalls, virus-scanning software, authentication technologies, and so on. As with any computer-based system, ultrasound systems require the level of protection typically provided by firewalls and other security devices between the medical system and any externally accessible systems. The U.S. Department of Veterans Affairs has developed a widely used isolation architecture for this purpose. Such perimeter and network defenses are an essential element of good security practices. The Department of Veterans Affairs *Medical Device Isolation Architecture Guide* is on this website:

http://www.himss.org/ResourceLibrary/ResourceDetail.aspx?ItemNumber=7236

Response to Product-Security Incidents and Malware Detection

In the event of a product-security incident, or if you detect malware (malicious software) on the system, immediately disconnect the system from the network and report the incident to your Healthcare IT Security department. Alternatively, report the incident by sending e-mail to:

productsecurity@philips.com

Security Issues and Guidelines

The following guidelines provide concrete examples of system and data vulnerabilities and methods for providing protection.

4535 619 41961_A/795 * FEB 2018

Philips

NOTE

Tools for central management of mobile devices are available to help facilitate the guidelines in this document and to help ease deployment, configuration, and security issues. Consult your organization's healthcare IT security department.

Device Requirements

Philips recommends starting with a device configuration that meets or exceeds the minimum requirements of the Lumify app, as well as the needs for security within your particular environment. The next step is to ensure the appropriate level of security controls are implemented in a manner that meets your local security policies as well as any applicable regulatory obligations.

Device Hardening

Similar in principle to OS hardening strategies utilized on desktop or laptops, device hardening involves the identification of all unnecessary functions and applications that are included within your device and disabling those functions or applications not required for your use. Depending on the device, this may also include disabling the ability of applications to perform background functionality that may impact the performance of your device while Lumify is in use. Device hardening reduces the attack surface of your device by eliminating those services that may become vulnerable over time.

Encryption

A key security control available on most Android devices is encryption. Encryption helps ensure that data stored on the system is protected and increases the strength of your access-control policies by rendering the data unrecoverable.

4535 619 41961_A/795 * FEB 2018

Philips

Network Security

Any networked ultrasound system must be connected to a secure local area network, one that provides protection against computer viruses and other harmful code or traffic. Ensure the local area network uses appropriate protection, such as only using secure wireless technologies, firewalls, intrusion detection and prevention systems, and vulnerability scanners.

Physical Access Control

Each healthcare organization should limit physical access to the ultrasound systems for the prevention of accidental, casual, or deliberate contact by unauthorized individuals. The organization safety or security office can provide more information about what measures are in place.

Position of Device

Unauthorized visual access to protected information can be minimized by positioning the device to prevent viewing from doorways, hallways, and other traffic areas. Initiate screen blanking by logging off the system or manually clearing the display before leaving the device unattended for any amount of time.

User Login and Logout Protections

A password protects saved protected health information (PHI) from unauthorized access, while meeting safety requirements for the device to be operational as soon as possible.

Taking into account the size and portability of tablet devices, implementing a password or passcode is critical to reduce the potential for exposing personal information if the system is misplaced or stolen. With some devices, additional controls may be implemented to wipe all data from the device if the password or passcode is entered incorrectly after a specified number of times. Those controls help enhance the standard access control model and help reduce the potential for exposing personal information.

For devices with login capabilities, a consistent user login process, including user names and passwords, provides good security for protecting information. In all cases, the healthcare organization must control access to the system.

Protective login and password practices include these:

4535 619 41961_A/795 * FEB 2018

Philips

- Implement strong passwords. This is the easiest and most-effective method to increase security. Strong passwords consist of at least eight alphanumeric, mixed-case characters and special characters, for example “@” or “*.” Never use words that can be found in a dictionary.
- Never post or share user names and passwords.
- Change passwords periodically.

Train system operators to log off of the system immediately after completing their work.

Information-Maintenance Example

This example of how to maintain information security uses a zone model of information flow.

Assumptions About the Environment

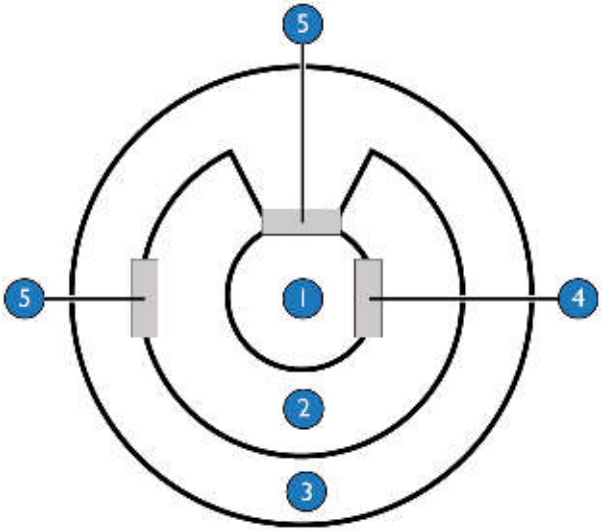
The ultrasound system relies on the healthcare organization to maintain a secure environment, with protection mechanisms for network access, encryption, and intrusion detection.

Information Zones

The information-flow model is commonly incorporated into security standards. An easy way to visualize this model is to diagram a healthcare organization as divided into three zones (see figure), with each zone having a different priority and level of use for the information. Some organizations decide not to extend their information to the farthest zone because they cannot guarantee its protection and integrity.

4535 619 41961_A/795 * FEB 2018

Philips



Security Solutions Between Zones

1	Zone 1: The ultrasound department
2	Zone 2: The rest of the healthcare organization
3	Zone 3: The Internet
4	Firewall
5	Firewall with IPSec

Zone 1: The Ultrasound Department

Most image transfer is performed within Zone 1. Backups, copies, and media containing ultrasound images must be carefully managed by department staff.

Zone 2: The Rest of the Healthcare Organization

Zone 2 includes clinics outside the department that have access to the system and, in some cases, the Internet. Proper authorization for access and use of audit trails is critically important.

4535 619 41961_A/795 * FEB 2018

Philips

Zone 3: The Internet

Zone 3 is used for connectivity to a HIPAA-compliant cloud-storage provider.

Security Between the Zones

Security between the zones should be managed by standard IT security solutions. Managers must be aware of the expected level of data traffic to choose a solution that is secure, yet does not act as a bottleneck in the information flow. Image distribution requires a high-bandwidth network.

Security Within the Zones

The security within the zones should be managed by a combination of standard IT security solutions and the security functions of the ultrasound system.

Security Protection Software

Lumify app updates are provided through regular releases and the Philips Field Change Order process.

Antivirus Scanning and Updates

The best protection against viruses is for a healthcare organization to establish an effective network-security policy.

Malware is responsible for many of the breaches that are making the headlines today. Traditional methods of malware protection include Anti-Virus (AV). Philips recommends choosing a reputable software package capable of meeting your malware protection needs. Additional steps can be taken to limit the potential for malware on your systems. This includes ensuring that any additional applications added to your device are from a reputable source. While applications may include malware, only installing applications necessary for the functionality of your device will help limit your risk of infection or breach.

4535 619 41961_A/795 * FEB 2018

Philips

Backups and Archives

CAUTION

The chosen export destination and mechanism must be in accordance with your local healthcare IT security policies.

You can export exams and images from the Lumify ultrasound system to a DICOM PACS, to a network share, or to a local directory. You can also send images by e-mail.

Backup Procedure

Ultrasound systems are designed to maintain information only as necessary to produce external documentation for medical records (such as films, traces, and printed records). If additional backup is necessary, establish an administrative protocol to archive all clinical studies before deletion.

Disaster Recovery Plans

It is your responsibility to ensure you have a disaster recovery plan that includes regular and complete patient data backup. Ultrasound systems are not long-term storage devices; patient data must be exported from the ultrasound system. For more information on exporting patient data, see your ultrasound system user information.

4535 619 41961_A/795 * FEB 2018

Philips

www.philips.com/healthcare

Philips Ultrasound, Inc.
22100 Bothell Everett Hwy
Bothell, WA 98021-8431
USA

EC REP

Philips Medical Systems Nederland B.V.
Veenpluis 4-6
5684 PC Best
The Netherlands

CE 0086

Published in USA
4535 619 41961_A/795 * FEB 2018 - en-US