PHILIPS

Ultrasound

Securing Lumify electronic protected health information on the Android platform

The highly mobile Lumify ultrasound solution puts the processing power normally found in traditional ultrasound carts into the transducer. Available on compatible Android smart devices, Lumify shatters the mold of the traditional ultrasound on-cart system by combining quality imaging with a hand-held fully kitted solution or bring your own device (BYOD) model.

Hand-held devices in healthcare typically need to support multiple security objectives including confidentiality, integrity and availability. To achieve these objectives, the security of mobile devices must provide a layered defense designed to protect against a myriad of known and unknown threats.

Objective

The purpose of this publication is to help you centrally manage the security of the mobile Lumify ultrasound solution. This publication explains typical security concerns inherent with hand-held devices, insights into the types of centralized management technologies available, and provides recommendations for securing mobile devices throughout their life cycles. The scope of this publication includes securing both organization-provided and BYOD Lumify mobile devices.

The most common information security requirements in the healthcare environment include:

- **Confidentiality** – ensure that transmitted and stored data cannot be read by unauthorized parties
- **Integrity** – detect any intentional or unintentional changes to transmitted and stored data
- **Availability** – ensure that users can access resources using mobile devices whenever needed

Philips recognizes that you can reduce the likelihood of data compromise through a combination of security features built into the mobile devices and additional security controls applied to the mobile devices and other components of the enterprise IT infrastructure.

This document does not attempt to recreate Android device or mobile operating system recommendations, which are widely available. Nor does this guide imply there is a single architecture that will address all of your security requirements. This guide assumes that your IT team has experience implementing security products within a healthcare organization and will create an infrastructure congruent with established standards and best practice in the healthcare IT environment.

The challenge

Medical devices have inherent challenges. While the primary focus has historically been on patient safety, information security has emerged as a serious need for medical institutions as well. Philips Ultrasound understands the need for security within the healthcare enterprise and has been working in close collaboration with our customers to meet these challenges.

Start with a strategy

Philips Ultrasound recommends starting with an Android tablet that meets the minimum requirements of the Lumify solution, as well as the needs for security within your particular environment. The next step is to design and implement security controls that are compliant with your local security policies and applicable regulatory obligations.

The design of the security controls uses a defense-in-depth strategy – the idea that a multilayered defense is more difficult to penetrate than a single barrier. It is the basis for best practices in medical device security. The layers can include security policies, procedures, access controls, technical measures, training and risk assessments. Your overall strategy should include the following elements:

- Integrated data at rest and data in transit protections
- Integrated virus, malware and host intrusion protections
- Integrated ports and protocol firewalling services

To protect your ultrasound investment, Philips recommends adopting a defense strategy that includes the following:

Mobile application integrity

A key defense is to limit where applications can be installed from. Google Play Store has a screening mechanism designed to prevent the introduction of malware into these distribution channels. Customers should consider prohibiting the download and installation of third-party applications onto the Philips Ultrasound Lumify device. If local security policy permits device users to install third-party applications, consider restricting the list of approved download sites to legitimate and official stores only (such as Google Play Store).

Additionally, carefully inspect the permissions requested by the apps you want to install onto your Android device. Practice the principle of least privilege and do not grant any third-party mobile application a higher level of permission than is required to perform its authorized function.

For compatible Android tablets that meet minimum requirements of the Lumify solution, please visit www.usa.philips.com/healthcare/sites/lumify/support/lumify-tablet-compatibility

Patch management

Unpatched vulnerabilities in the device operating system (OS) are a common escalating and contributory risk factor. Always keep your OS and all software up to date. Android devices running with outdated software and OS are more susceptible to cyberattacks. Not only should the mobile operating system be kept updated, steps should be taken to ensure that genuine updates are applied.

Device hardening

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

Malware protection

Malware is responsible for many of the breaches that are making headlines today. Traditional methods of malware protection include antivirus protection. Philips Ultrasound recommends choosing a reputable software package capable of meeting your malware protection needs. Consider solutions that move beyond traditional signature-based detection, such as solutions that use behavior-based algorithms to detect inappropriate actions by applications and correlate this information to build a reputation database for otherwise uncategorized applications.

Access controls

Taking into account the size and portability of tablet devices, implementing an authentication scheme is critical to reduce the potential for exposing personal information if the system is misplaced or stolen. Many Android devices offer a variety of authentication mechanisms, including:

- Password (use complex schemes)
- Passcodes
- Pin entry (use 6-digit at a minimum),
- Pattern of dots
- Biometrics – check the device manufacturer's user manual to remain abreast of technology limitations (e.g., Samsung's IRIS scanner is limited to a single user per device)

Customers may also consider more robust forms of authentication. Examples include token-based authentication, network-based device authentication and domain authentication, in addition to the built-in device authentication capabilities.

With some Android 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 (typically 10). These controls help enhance the standard access control model, help reduce the potential for exposing personal information, and help protect the organization from potential privacy breaches.

Patient data security

Another key security measure available on most tablet devices is encryption. Physical possession is still the most viable path to data collection. On tablets, encryption helps ensure that data stored on the tablet remains protected from authorized disclosure and increases the strength of your access control policies by rendering the data unrecoverable, thus reducing the risk of a stolen tablet resulting in a reportable incident.

Philips recommends customers deploy supplemental security controls as risk merits, for example, antivirus software and data loss prevention technologies.

Mobile device management (MDM)

MDM software allows management and distribution of apps, configuration and security settings, monitoring for malware, patching firmware and apps, and containerization of business data. While the functionality of each specific MDM solution may vary, an MDM provides administrators the ability to manage, monitor and secure their mobile devices. Some of the specific capabilities of MDM include the following:

- Hardware inventory
- Application inventory
- OS configuration management
- Restriction or removal of the ability to utilize email and web-browsers
- Implementation of kiosk mode
- Mobile app deployment, updating and removal
- Mobile app configuration and policy management
- Remote view and control for troubleshooting
- Remote actions, such as remote wipe
- Mobile content management

Customers may also consider employing an MDM solution to achieve overall enterprise needs, such as:

- Centralized policy enforcement
- Management and configuration of business functionalities
  - Intranet services
  - Email access
  - Remote data wipes (to provide data protection if a device is lost or stolen)

Network security

The Lumify solution provides customers with the ability to overcome many risks associated with the use of wireless and cellular networks through increased configuration and control of the mobile device security. Because Lumify utilizes a BYOD model, customers are able to choose both the mobile device and the mobile device security settings to successfully achieve the necessary balance between overall enterprise security, patient data security, and the intended use case for their Lumify solution.

Additionally, the risk from the use of untrusted networks can be reduced by using strong encryption technologies (such as virtual private networks) to protect the confidentiality and integrity of communications, as well as using mutual authentication mechanisms to verify the identities of both endpoints before transmitting data. Another possible mitigation includes prohibiting the use of unsecure Wi-Fi networks, such as those running known vulnerable protocols. Furthermore, all network interfaces not needed by the device can be disabled, thus reducing the attack surface. Consider leaving the Wi-Fi disabled so network communication passes over the cellular network, which is harder to impersonate.

Use threat models

Philips Ultrasound recommends that customers develop threat models for both mobile devices and the resources accessed through these systems. Mobile devices often need additional protection because their use places them at higher exposure to threats than other client devices.

Before designing and deploying mobile device solutions, organizations should identify the device's intended use and which patient data, if any, will pass through that device. This will help your team develop a solid threat model. Threat modeling helps organizations to identify security requirements and to design the mobile device solution to incorporate the controls needed to meet the security requirements.

Philips Ultrasound recognizes the importance of securing your medical devices and protecting your patient data. Together, we strive to maintain a secure environment by remaining vigilant and identifying the ever-changing cybersecurity threat landscape. We are committed to meet the needs and requirements of our customers.

Additional resources

For more information about patient data protection, see Shared Roles for System and Data Security on your User Information CD. It contains guidelines to help you understand security recommendations for your Philips system. You can also find information in the Support section of the Lumify portal: www.philips.com/lumify

Additional links

NIST SP 1800-1 Securing Electronic Health Records on Mobile Devices
https://www.nccoe.nist.gov/publication/1800-1/VolC/index.html#hosts-and-mobile-device-security

NIST, NCCoE Publish Guide on Healthcare Mobile Device Security
https://healthitsecurity.com/news/nist-nccoe-publish-guide-on-healthcare-mobile-device-security

How Mobile Healthcare Users Affect the Industry, Data Security
https://healthitsecurity.com/news/how-mobile-healthcare-users-affect-the-industry-data-security

www.philips.com

Printed in The Netherlands.
4522 991 46141 * MAR 2019