PHILIPS

Ultrasound

Security

Are you **protecting** your medical equipment from patient data breaches?

Like every industry that relies on increasingly connected computer networks, the healthcare industry is faced with a growing number of security breaches.

Lisa Gallagher, senior director of privacy and security for Healthcare Information and Management Systems Society (HIMSS), estimates that between 40 million to 45 million patient records have been compromised in HIPAA data breaches.[1] Although this number is an estimate because not all breaches are reported, another study suggests that breaches of health records jumped 138 percent from 2012 – 2014.[2]

Whether these breaches are caused by hackers, malware, or are instances of unauthorized access, they present a threat to patient safety and data security. In addition, the cost of healthcare breaches can exceed several millions of dollars, and that cost can be compounded by civil suits and other legal actions, as well as the damage caused to an institution's reputation.

The challenge for imaging devices

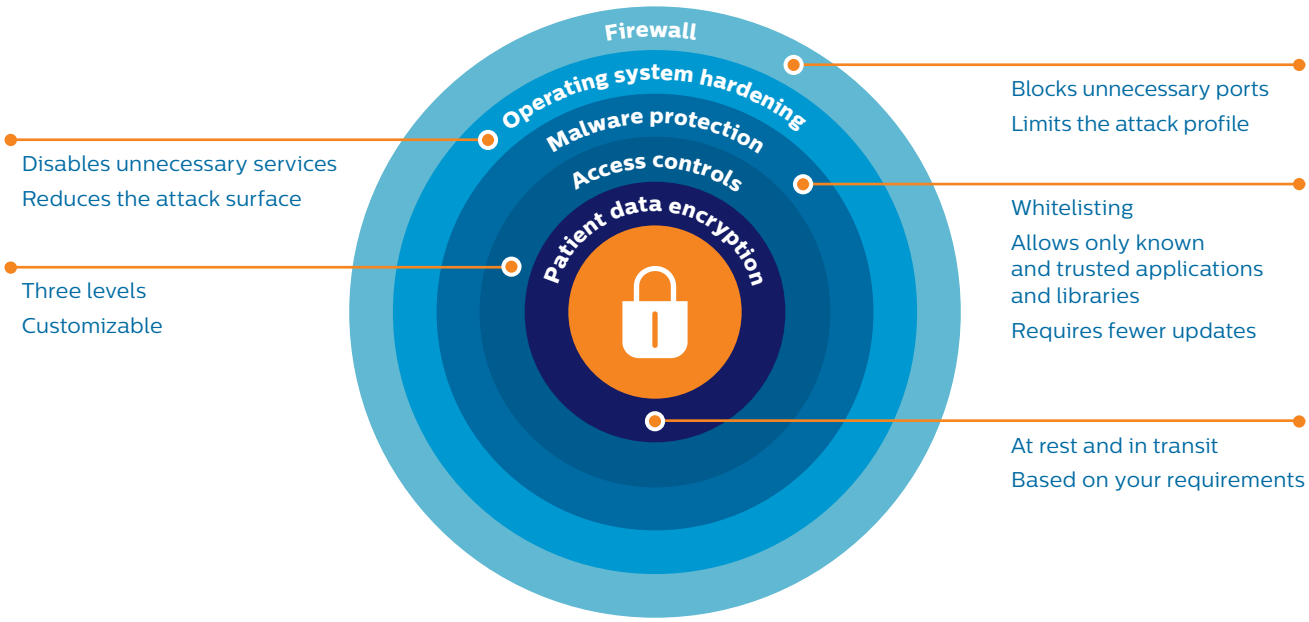
Imaging devices are not immune to these attacks. Most were developed with a focus on clinical utility, with little regard to the fact that they are also computers on a network that can be exploited for illegal purposes. This leaves medical devices vulnerable, and attackers are able to use these closed medical devices as pivot points within the healthcare network. In addition, the sheer number of networked medical devices makes maintaining cybersecurity a daunting task. HIMSS concludes that "Hospitals and similar healthcare organizations typically have 300% to 400% more medical equipment than IT devices."[3] As a result, the FDA has issued guidance on cybersecurity for networked medical devices.[4]

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

Starting with the **right strategy**

Defense-in-depth strategy, the idea that a multi-layered defense is more difficult to penetrate than a single barrier, 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.

Defense-in-depth strategy



Addressing security in EPIQ and Affiniti products

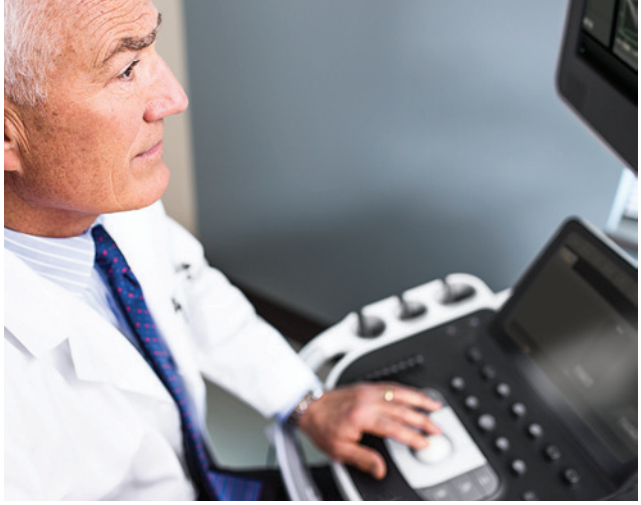
Philips Ultrasound has applied the principle of the defense-in-depth strategy to its EPIQ and Affiniti ultrasound systems, implementing a security strategy that comprises five layers:

- Firewall
- Operating system hardening
- Malware protection
- Access controls
- Patient data encryption

Each of these layers plays an important role in helping you thwart hackers, defend against malware, and prevent unauthorized access.

Firewall blocks unnecessary ports

Strict firewall policies that block all unnecessary ports inhibit communication with unauthorized computers, limiting the attack profile that a malicious hacker may try to exploit.



Operating system hardening disables unnecessary services

Similar in principle to firewalls, operating system (OS) hardening involves identifying all unnecessary services and functions that are included within the operating system and disabling those not required by the ultrasound systems. OS hardening reduces the attack surface by eliminating those services that may become vulnerable over time. Philips follows the Standard Technical Implementation Guides (STIGs) provided by the Defense Information Systems Agency (DISA).

Malware protection via whitelisting provides low maintenance protection

The traditional method of malware protection, anti-virus (AV) software, requires frequent updates to stay current with new viruses and malware being released every day. Hospitals risk being attacked before AV software has addressed new malware.

To mitigate this risk, Philips has implemented the McAfee Application Control solution. This solution, known as whitelisting, protects your EPIQ and Affiniti systems from malware by allowing only known and trusted applications and libraries to function. Because whitelisting doesn't require constant updating like traditional AV software, it requires less maintenance and fewer updates.

Access controls can be adapted to your needs

It is estimated that 22% of security breaches since 2009 were due to unauthorized access.[2] To help you control access to data on your ultrasound systems, with EPIQ and Affiniti you can choose from three access control levels:

- **No restrictions (default level):** A clinical user may perform exams and access any previously completed exams stored on the system without requiring a login.
- **Only patient data is locked:** Each user must enter valid credentials prior to accessing the previously completed exams, but an emergency exam may still be performed without requiring a user login.
- **Complete system is locked:** Each user must successfully log in before performing a scan or accessing patient information.

Patient data encryption at rest and in transit

All patient data stored on the EPIQ and Affiniti hard drives can be encrypted according to your institution's specific requirements. In addition, you can choose DICOM with TLS for node authentication without encryption, DICOM utilizing TLS encryption, or a combination of the two to encrypt patient data in transit. (This requires corresponding functionality on your PACS system.)

User management simplifies account maintenance

With EPIQ and Affiniti you have the ability to create multiple clinical user accounts and multiple hospital administrator accounts. With both systems, hospital administrators have the option of specifying password policies in accordance with local information security requirements and policies. EPIQ and Affiniti systems can interface with your LDAP environment to authenticate users and groups using your standard network accounts (i.e., Active Directory).

Audit logging provides data for analysis

Philips Ultrasound has enhanced EPIQ and Affiniti systems' audit logging capabilities. Users can configure the system to send the logs to a local system log (syslog) server for retention, accessibility, and further analysis. To aid forensic analysis, users can ensure consistent time stamps by synchronizing the time on the ultrasound systems with your network time server.

Security-related options

Core features

- Firewall policy blocks all unnecessary ports
- OS hardening
  - OS settings utilizing the DISA STIGS
  - Disabled unnecessary services
  - Disable auto-run for removable media
- Media export security
  - Provides the ability to disable export of patient data to removable media

Safeguard (purchasable option)

- Malware protection utilizing the McAfee Application Controls whitelisting solution

Security Plus (purchasable option)

- Access level
  - No restrictions – users may perform exams and access all previously completed exams or MWL data
  - Only patient data is locked – users may perform exams without requiring a login, but must successfully log in prior to accessing previously completed exams or MWL data
  - Complete system is locked – users and administrators must successfully log in prior to any system access
- User management policy
  - User management local
    - Local user management
      - Support for multiple unique user accounts
      - Support for multiple unique administrator accounts
  - User management remote
    - Supports active directory authentication utilizing LDAP (system may not be joined to the domain)
      - Support for individual accounts or AD groups for users and administrators
      - May utilize LDAP or secure LDAP
      - Customer may configure the system to perform authenticated binding
- Password policies
  - Provides the ability to specify password policies for local accounts
    - Password history (1-8)
    - Minimum password length (6-14 characters)
    - Maximum password length (6-63 characters)
    - Minimum password age (0-998 days)
    - Maximum password age (1-999 days)
    - Password complexity
  - Account lockout policies
    - Lockout threshold (1-999 minutes)
    - Lockout duration (1-999 minutes)
    - Lockout counter reset (minutes)
- Auto logoff – automatically logs off a user after the specified period of inactivity
  - Disabled, 5, 10, 20, 30, or 60 minutes*
- Hard drive encryption
  - 128 bit
  - 128 bit with diffuser
  - 256 bit
  - 256 bit with diffuser
- Login/legal banner
  - Configurable login/legal banner
  - Configurable login/legal banner title
- Audit log export
  - Audit logs may be exported utilizing syslog
    - Available protocols are UDP or TLS

*Will pause an active exam

1. Gallagher L. Presentation. 2012 Boston Privacy and Security Forum.
2. McCann E. HIPAA data breaches climb 138 percent. Healthcare IT News. February 6 2014.
3. Medical Device Security. Healthcare Information and Management Systems Society. http://www.himss.org/resourcelibrary/TopicList.aspx?MetaDataID=1581
4. Guidance for Industry - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software. U.S. Food and Drug Administration. http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077812.htm

www.philips.com/ultrasound

Printed in The Netherlands.
4522 991 16001 * NOV 2015