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.

The HIPAA Journal published that in 2021, according to the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR), 712 healthcare data breaches were reported, which equates to approximately 45,706,882 healthcare records that were exposed.[1] The latest IBM Cyber Security report from 2022[2] showed healthcare as the sixth-most attacked industry, with 38% of attacks contributed to ransomware. This is a higher percentage than most other industries.

Whether these breaches are caused by hackers, malware, or 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 by the damage caused to an institution's reputation.

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.

The challenge for imaging devices

Imaging devices are not immune to these attacks. Historically, these were developed with a focus on clinical utility, with little regard to the fact that networked computers, such as laptops and workstations, can be exploited. This would leave medical devices vulnerable to data breaches, malware, ransomware and general cybersecurity attacks as a part of the healthcare institutions' digitalized infrastructure. Philips Ultrasound recognizes this shift, the importance of facilitating the safe and secure use of medical devices, and the continuous focus on cybersecurity by regulatory frameworks. Together, we can maintain secure environments that secure your medical devices, protect your patient data, and mitigate attacks by remaining vigilant and identifying the ever-changing cybersecurity threat landscape. To assist the healthcare industry, the FDA has issued guidance on cybersecurity for networked medical devices.[3]

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

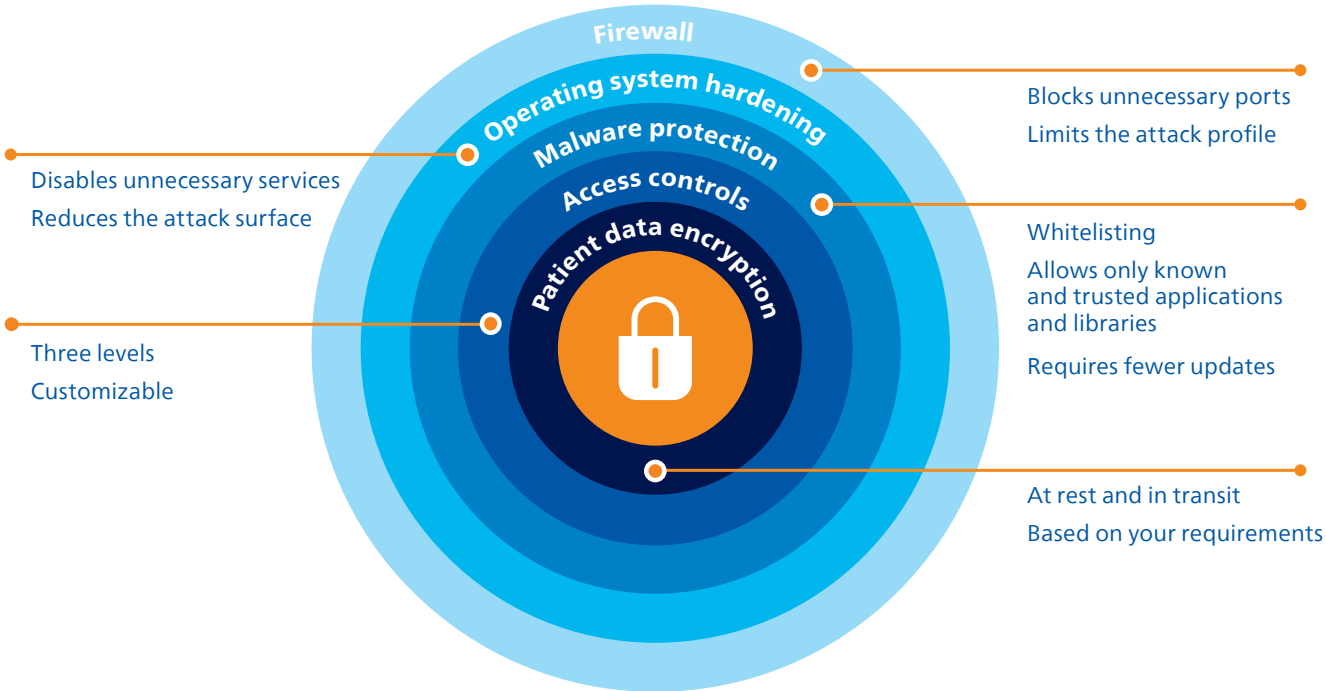
Philips Ultrasound has applied the principle of the defense-in-depth strategy to its EPIQ and Affiniti ultrasound systems, implementing a security strategy that comprises five layers:

- **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 OS 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.

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 communication 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.

Access controls can be adapted to your needs

According to the Healthcare Information and Management Systems Society (HIMSS), unauthorized access controls are implemented in 34% of organizations.[4] To help you control access to the ultrasound system and its associated data, EPIQ and Affiniti allow you to 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.

Security-related options

Core features

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

Safeguard (optional)

- Malware protection utilizing the McAfee Application Controls whitelisting solution

Security Plus

- Access level
  - No restrictions: users may perform exams and access all previously completed exams or Modality Worklist (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
  - 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 passwords)
    - 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 attempts)
    - 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
  - Bitlocker 256 bit
- Secure transmissions (using TLS 1.2)
  - Secure DICOM will encrypt your DICOM communication traffic
  - Secure LDAP will encrypt your authentication credentials
  - Secure Philips Remote Support (PRS)
  - Syslog transmission
- 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.

References

1 December 2021 Healthcare Data Breach Report. HIPAA Journal. www.hipaajournal.com/december-2021-healthcare-data-breach-report

2 July 2022 IBM Security, Cost of a Data Breach Report 2022. www.ibm.com/reports/data-breach

3 Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software – Guidance for Industry. January 2005. www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-networked-medical-devices-containing-shelf-ots-software

4 Healthcare Information and Management Systems Society. 2021 HIMSS Healthcare Cybersecurity Survey

www.philips.com

Printed in the Netherlands.
4522 991 80531 * APR 2023