PHILIPS

Emergency Care Informatics Suite

Security

Security woven into every layer of your emergency care solution

Philips uses secure-by-design and defense-in-depth approaches to secure your emergency care solution. This summary details these approaches and the solutions that make up our multi-layered system that protects data confidentiality and system integrity.

The challenge

Advances in communicating across the continuum of care demand an equally sophisticated security strategy

It may be surprising that, for all its benefits, the revolution in connected health devices is still in its infancy. Ever-more sophisticated devices and solutions are achieving higher-order goals of user-friendliness for clinicians and assisting staff. Breakthroughs that enhance clinical outcomes are now embedded in procedure efficiency with smoother workflows, bringing relevant data directly into the continuum of care.

The far-reaching benefits of connected emergency care solutions translate into an evolved strategy for security and privacy. Increasing sophistication means that hackers have more ways to enter your system, while incentives for them to do so are also increasing. Recent studies suggest that confidential patient data is 50 times more valuable on the black market than financial data.[1] This means that your goal of providing excellent levels of care provides criminals with an opening to manipulate your data.

Because our goal is a secure continuum of care within emergency care solutions that serve clinicians and patients, we have created security solutions that serve those outcomes.

Philips Emergency Care Informatics Suite (ECI) recognizes the importance of securing medical devices and protecting your patient data. Together we can maintain a secure environment by remaining vigilant and identifying the ever-changing security-threat landscape. Because we are committed to meeting the needs and requirements of our customers, our security plans encompass your people, processes and technology with the goal of ensuring the confidentiality, integrity and availability of critical data – whether at rest or in transit.

The mindset

Secure by design – Philips Secure Development Lifecycle (SDLC)

Industry trends have shown that cyber-attacks are moving to the application layer of products and pose a significant threat to customers and patient information over the Internet of Things (IoT). According to data collected by the Internet Storm Center, over 70% of attacks on networks are against the application layer.*

We strengthen the resilience of our products and services by applying capabilities, components and techniques within the software development process.

Leveraging this methodology, requirements and controls are addressed at each phase of the secure development lifecycle, including the use of Product Security Risk Assessment (PSRA), Data Protection Impact Assessment (DPIA) processes, static code analysis, ethical penetration testing, and continuous product security training across the Philips organization.

While tools and processes are key to the Philips SDLC, secure by design is a mindset that requires an end-to-end approach that begins with architecture and high-level design and progresses to coding, testing and post-market support.

The strategy

Defense in depth

Your hospital personnel are likely well-acquainted with the Swiss Cheese Model of patient safety, whereby cumulative acts prevent threats to patients' lives. Defense in depth is precisely the same strategy: even if one layer fails, several others will counter the attack, preventing penetration from attacks that arise from diverse vectors.

A multi-layered defense is more difficult to penetrate than a single barrier (Figure 1, page 4), and 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. By default, many of these control layers are built into the platform. For others, we work with you to implement them and optimize your protection of patient data.

Standards

The Philips Product Security Risk Assessment (PSRA), is built on IEC 80001, and the Philips Services Security Risk Assessment (SSRA) is built on the ISO 27001 and NIST 800-53.

ECI was risk-assessed against these well-known and established security frameworks and standards.

Key features

- **Physical security incorporating regional redundancy**
- **Data in transit from HeartStart Intrepid provisioned through an SSL Certificate using transport layer security TLS 1.2**
- **Industry-standard AES 256-bit encryption at rest**
- **Backup policy allows point-in-time restoration up to the last 15 minutes**
- **Multi-tiered network security provides granular access configuration**
- **Penetration-tested against industry standards**

What is Emergency Care Informatics Suite?

Philips ECI is a cloud-based software platform consisting of applications to support emergency care, whether that care is from Emergency Medical Services (EMS), hospital personnel or lay responders. We recognize the need to comply with the latest privacy and security standards and scrutinize the platform and applications to ensure compliance.

* https://isc.sans.edu/ and The Internet Storm Center is a program of the SANS Technology Institute, a branch of the SANS Institute which monitors the level of malicious activity on the Internet, particularly with regard to large-scale infrastructure events.

[1] Personal health information is 50 times more valuable on the black market than financial information according to Cybersecurity Ventures, and stolen patient health records fetch upwards of $50 per record (10 to 20 times more than credit card information). Alterson G. Confronting One of Healthcare's Biggest Challenges: Cyber Risk. Forbes. 2019(04). www.forbes.com/sites/insights-intelai/2019/02/11/confronting-one-of-healthcares-biggest-challenges-cyber-risk/.

Layers in unison

Each layer of the defense-in-depth strategy is an effective component in itself. However, their cooperation optimizes your organization's cybersecurity, limiting degrees of risk.

Penetration and vulnerability testing

The Philips Security Center of Excellence (SCoE) team conducts penetration and vulnerability testing to independently verify that Emergency Care Informatics has effective protection. It reviews Web Application Security Assessment OWASP Top Ten – 2017, a common software category for vulnerability classification. Comprehensive security scanning and testing use Fortify and Black Duck to validate software security.

Health Suite Digital Platform and Amazon Web Services

ECI utilizes Philips Health Suite Digital Platform (HSDP), which is built on Amazon Web Services (AWS).

Customer data is stored in AWS data centers considering data residency regulatory requirements (See table below). Contact the Philips Emergency Care business unit if you have questions about data centers for your location.

Country or region	Data center
APAC	Australia
Japan	Japan
EU	Ireland
LATAM	United States
Canada	Canada
Africa	Ireland
United States	United States
United Arab Emirates	United Arab Emirates

Data security

For connected devices, data in transit to ECI is encrypted using AES 256 with RSA key. Azure Cloud Service, as well as the HSDP and ECI teams, continually monitors the service.

All communication uses TLS protocol version 1.2 or higher. All inbound communications to the application are via secure HTTPS port 443; all other ports are disabled. Data at rest is encrypted using industry standard AES 256-bit encryption.

Application authorization model

Access to ECI and the supporting infrastructure is strictly controlled. Only a limited number of full-time Philips employees with privacy and security training are super-administrators. Their primary function is to deploy security updates to the service, and notify the customer Technical Contact of outages, upgrades or changes to the system. Also serves as the final escalation path for customer account issues. At no time is personal data exposed to a Philips super-administrator. The Philips super-administrator is responsible for patching the system with the latest security updates, which are released monthly.

The customer IT administrators are responsible for user account set-up and administering roles to a user. Users can have multiple roles if the customer administrator assigns them.

The ECI and applications include security protocols to enable the secure handling of data – passwords must satisfy strong password requirements and expire after 90 days, sessions time out after twenty minutes, and audit logs are kept.

Data backup

Data is backed up via infrastructure and database backups. Data is backed up before and after receiving system software patches, as well as before and after application software upgrades or version changes conducted via the cloud. Critical databases are backed up frequently to ensure data is able to be restored up to the last 15 minutes. The data retention period is 30 days.

AWS physical security

AWS is the world's largest cloud services provider. AWS data centers are surrounded by three physical security zones and a range of electronic intrusion detection systems. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, access is immediately revoked, even if the employee continues employment at Amazon or Amazon Web Services. All physical access to data center by AWS employees is logged and audited routinely. Zone 1 (the outer perimeter) is a fence that is either crash-rated to prevent a vehicle from penetrating it or backed by state-of-the-art Jersey barriers. Zone 2 (electrical systems and generators) requires both a badge swipe and a pin to access. The only entrants are authorized engineers. Each door is under video surveillance with the feed monitored both locally and remotely.

The space between perimeters is studded with internal trip-lights that are also monitored and managed around the clock. Zone 3 (data servers and networking) requires another badge swipe and pin for entry. The buildings are also equipped with metal detectors. No transportable media (such as USB keys) are allowed in or out of the building.

Fire detection and suppression

Automatic fire detection and suppression equipment is installed to reduce risk. The fire detection system utilizes smoke detection sensors in all AWS data center environments.

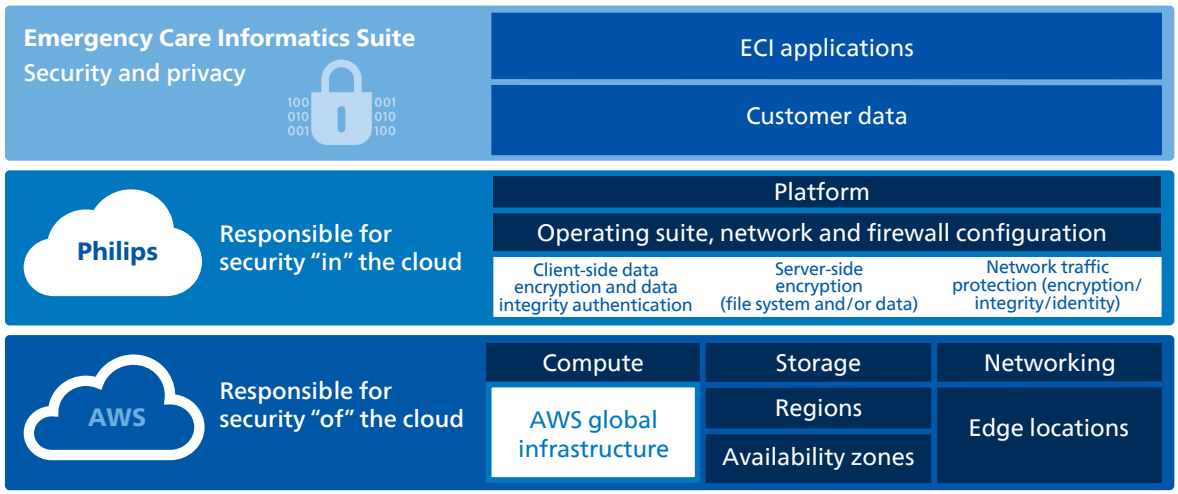
Power

The electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day and seven days a week. Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure. Generators are used to provide backup power for the entire facility.

Climate and temperature

Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages.

Figure 1 **Multi-layered system that protects your data confidentiality and system integrity**



Commitment

Continuous security and privacy development

Philips continues to examine and re-engineer existing products to best accommodate the requirements of our security-minded customers. We are deeply engaged in creating the products of tomorrow based on fundamental security principles.

We will continue to work closely with providers, IT organizations and customers to provide flexible solutions to today's problems, even as we create new securely designed products.

For more information on Privacy, please visit our website.

For more information on how Philips complies with security standards, please visit:
https://www.usa.philips.com/healthcare/about/customer-support/product-security

Emergency Care Informatics Suite
Philips Medical Systems
22100 Bothell Everett Highway
Bothell, WA 98021-8431, USA

www.philips.com

Printed in the Netherlands.
4522 991 79631 * OCT 2022
LC2272-014-029