PHILIPS

Healthcare Informatics

Security matters to you and to us

The intersection of devices, health apps, and platforms creates unprecedented potential to transform healthcare and enable better care at lower cost. But as healthcare data proliferates, so does the need for vigilance.

Healthcare data is:
#1 target for cybercriminals

10× more valuable than credit card data alone

More connections can mean more risk

The growing interconnectedness of devices and systems leads to greater vulnerability to cybercrime:

- As hospitals merge, they are linking many different systems, making security even more challenging
- Most medical devices and systems don't support the standard IT practices designed to keep them secure, so breaches can happen more frequently

Security is our ongoing responsibility and is one we take seriously as an organization.

Getting ahead of the risks

Security threats evolve rapidly and continuously, so we try to anticipate the risks — proactively working toward solutions for problems that may be on the horizon.

Philips security by design

Our end-to-end approach to security for software and data

At Philips, we design security from the inside out and from end to end so customers can rely on the integrity of our services, software, solutions, and partnership.

We infuse security principles from the start — beginning with product design and development through testing and deployment. We stay committed to security by adhering to robust policies and procedures for monitoring, effective updates, and, where necessary, incident response management.

We work to support the confidentiality, integrity, and availability of your software and data, fortifying them against exposure to the "three deadly sins":

Lack of strong identity management

Encryption risk

Software obsolescence and ineffective patch management

Valuable resources

Visit the links below to learn what experts have to say about healthcare cybersecurity and brush up on the most recent government recommendations and rulings.

- HHS.GOV on Cybersecurity Task Force Report 2017
- FDA 21 CFR Part 820 — Quality System Regulation Is the FDA Control Structure for Medical Devices
- NIST 800-53 Security and Privacy Controls for Information Systems
- Healthcare Information and Management Systems Society (HIMSS) — Medical Device Security

Our security efforts also include:

- Implementing security hardening based on the US Department of Defense Security Technical Implementation Guides
- Partnering with industry groups, governmental regulators (US and others), and healthcare providers to develop new standards
- Conducting risk assessments, source code analysis, and vulnerability and penetration testing
- Vulnerability information sharing

> "Product and information security is a combination of education, policies and procedures, physical security, and technology."

Michael McNeil
Head of Global Product & Security Services, Philips

Secure your solutions to protect your patient information, reputation, and bottom line.

- Read our full position paper and learn more
- Call your local Philips Healthcare Informatics Representative, visit www.philips.com/productsecurity, or email us at productsecurity@philips.com

PHILIPS

www.philips.com

4522 991 44301 * DEC 2018