PHILIPS

Patient monitoring

Product security


# Philips Patient Monitoring Systems: Our approach to protecting patients, medical devices and information

## Over 100 million patient healthcare records were breached last year

Last year's global cyber-attack hit the National Health Service (NHS) hard. Hackers blocked access to data and then held it ransom. Healthcare organizations paid these hackers $54,000 for access to their own patient information.*

Whether it's ransomware, malware or a vendor who lacks system updates and patching support capabilities, healthcare is the number one cyber-attacked industry. This is because most medical devices don't support the standard IT practices designed to keep them secure, so breaches happen more frequently.

**$200** cost per patient record of a **healthcare breach**.

**vs.**

**$8**** cost per patient record **to prevent a breach**.

**Your medical devices need a serious cyber check-up.**
Philips Patient Monitoring is a regulated medical IT system that provides continuous monitoring and communication of patient vitals while meeting manageability, serviceability and security requirements. The following medical devices are included in our security solution:

- Patient Information Center iX (PIC iX) B.02 and higher
- IntelliVue Bedside Monitors Release M and higher
- IntelliSpace Critical Care and Anesthesia (ICCA)
- CareEvent B.01 and higher
- IntelliSpace Perinatal (Integration Test only)
- CompuRecord (Integration Test only)

* Elliptic, WannaCry tracker, Rowland Manthorpe, May 15, 2017, http://www.wired.co.uk/article/nhs-hackers-bitcoin-value.

** According to a PwC Health Research Institute analysis.

# Philips patient monitoring security solutions

- **Lifecycle Management**
  When new software or an operating system releases, we publish the end of support dates for the legacy product you are using. This allows you time to budget, plan for upgrades and prevent the risk of unsupported medical devices and operating systems.
- **Securing clinical network**
  We provide best-practice, product-specific security recommendations to effectively secure IntelliVue Patient Monitoring System's wired and wireless devices.
- **Generate confidence with IT stakeholders**
  Philips PIC iX System implements security hardening based on the US Department of Defense (DoD) Security Technical Implementation Guides (STIGs). The applicable STIGs, includes, but is not limited to: Windows® operating system, .NET, SQL and Internet Explorer.® System hardening includes planning, testing, implementing and auditing patch management software and protecting against vulnerabilities disclosed by the manufacturer.
- **Security assessment and penetration testing**
  Using two types of testing, we access system vulnerability and measure which flaws will leave the system open to the most risk. Includes product-specific NESSUS® scans and penetration testing.
- **Active Directory authentication and authorization**
  By leveraging Active Directory PIC iX inherits customer authentication and password policy settings. This improves authentication and authorization.
- **Strict configuration management process**
  Integrity assurance through a product's lifecycle by making the development and deployment process controllable and repeatable.
- **Network management**
  Our management system consists of authentication, authorization and accounting (or AAA) and includes the following recommendations:
  - Employ logging methods for global network configuration access/change audits. These methods track not only configuration change times, but also the user ID making the change.
  - Utilize AAA services, such as TACACS+ or RADIUS.
  - Configure all user accounts to automatically time out.
  - Enlist secure protocols (HTTPS, SSH, SNMPv3, etc.) for system management and disable unsecured protocols (HTTP, Telnet and SNMP) where possible.



# Valuable resources

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

**HHS.GOV on Cybersecurity Task Force Report 2017**

**NIST 800-53 Security and Privacy Controls for Information Systems**

**FDA 21 CFR Part 820 – Quality System Regulation is the FDA Control Structure for Medical Devices**

**Healthcare Information and Management Systems Society (HIMSS) – Medical Device Security**

## Secure your medical devices in order to protect your patient information, reputation and bottom line.

Call your local Philips Patient Monitoring Sales Representative, visit **www.philips.com/productsecurity** or email us at **productsecurity@philips.com**



www.philips.com

4522 991 36401 * JUN 2018