PHILIPS

Patient monitoring

Improving the prognosis for **healthcare cybersecurity**

Philips patient monitoring education, risk management and clinical network cybersecurity

IT experts are all too familiar with security threats from ransomware, phishing and cybertheft. Yet, securing regulated medical devices requires a totally new set of processes, approvals and collaboration.

Understanding and applying risk management practices

By adopting risk management best practices, we can help your hospital avoid potential cyberthreats and mitigate risks.

- **Patient monitoring devices – a portal for cybercrime.** Hackers are attracted to healthcare, because the industry tends to lag others in terms of cybersecurity. According to Beazley – a global cybersecurity insurance company – 45 percent of all ransomware attacks it studied in 2017 targeted healthcare organizations.[1] On the black market, medical information is worth ten times more than credit card numbers.[2]

  One of the easiest ways that hackers gain access to sensitive patient HIPAA or PHI information, is through patient monitoring devices. Because these devices are connected to sensors and monitors, they're also entry points for larger hospital networks.

  Antivirus protection. Any time you modify a regulated medical device – which includes installing an antivirus application – it requires validation. Unless it's re-verified after installation, your medical devices are not considered to be safe or secure.

- **Including the right stakeholders.** Cybersecurity is not just the domain of the IT experts, especially when it comes to healthcare. To make our customers more cyber-secure and efficient we encourage teamwork and collaboration. To be successful, clinical, biomed and executive-level stakeholders also need to have a seat at the table, providing their insight and guidance. Making a cybersecurity decision that can impact staff, patients and your hospital's future, is an important and serious step. Figure 1 shows the recommended key stakeholders.

- **Stakeholder responsibilities.** We recommend creating responsibility agreements (contracts) to help drive accountability and streamline workflow.

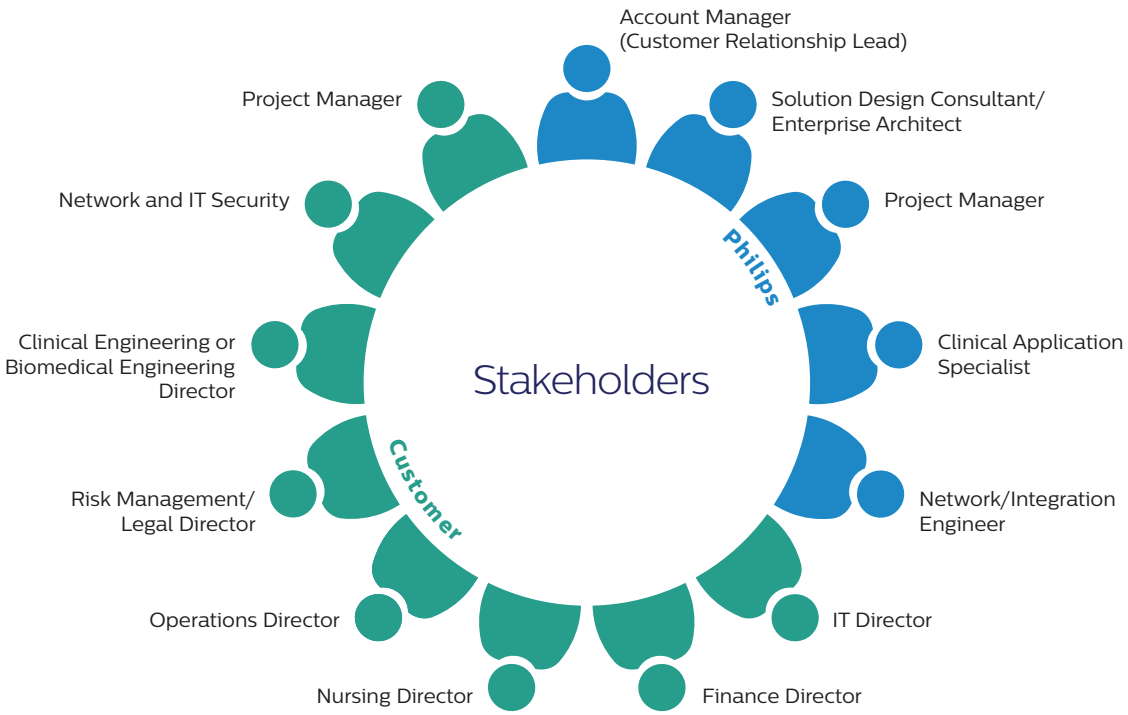


Figure 1: Recommended key stakeholders.

Clinical and IT requirements

Patient monitoring and clinical networks must work together to support safety standards and cybersecurity efforts. The Philips integrated patient monitoring solution must interface with numerous patient care devices and hospital systems.

The reference architecture diagram, figure 2, illustrates how the Clinical and IT requirements for the hospital converge to support customers and their caregiving needs.

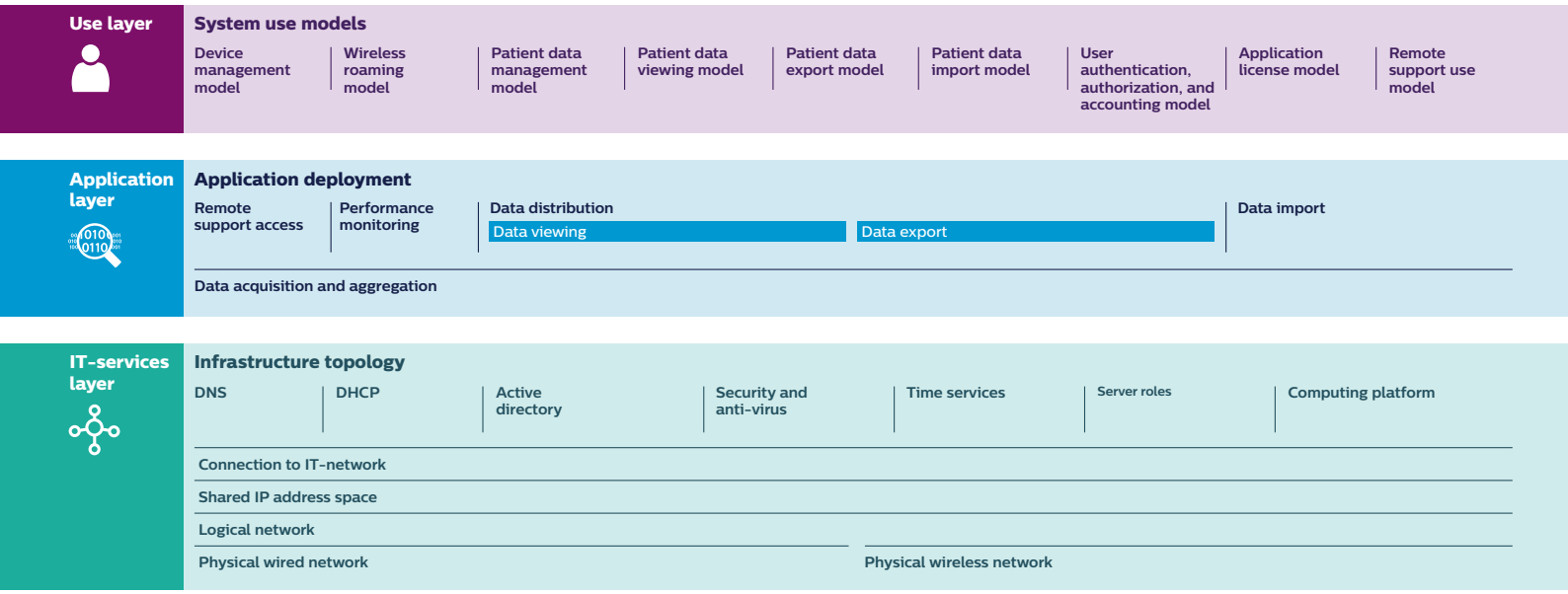
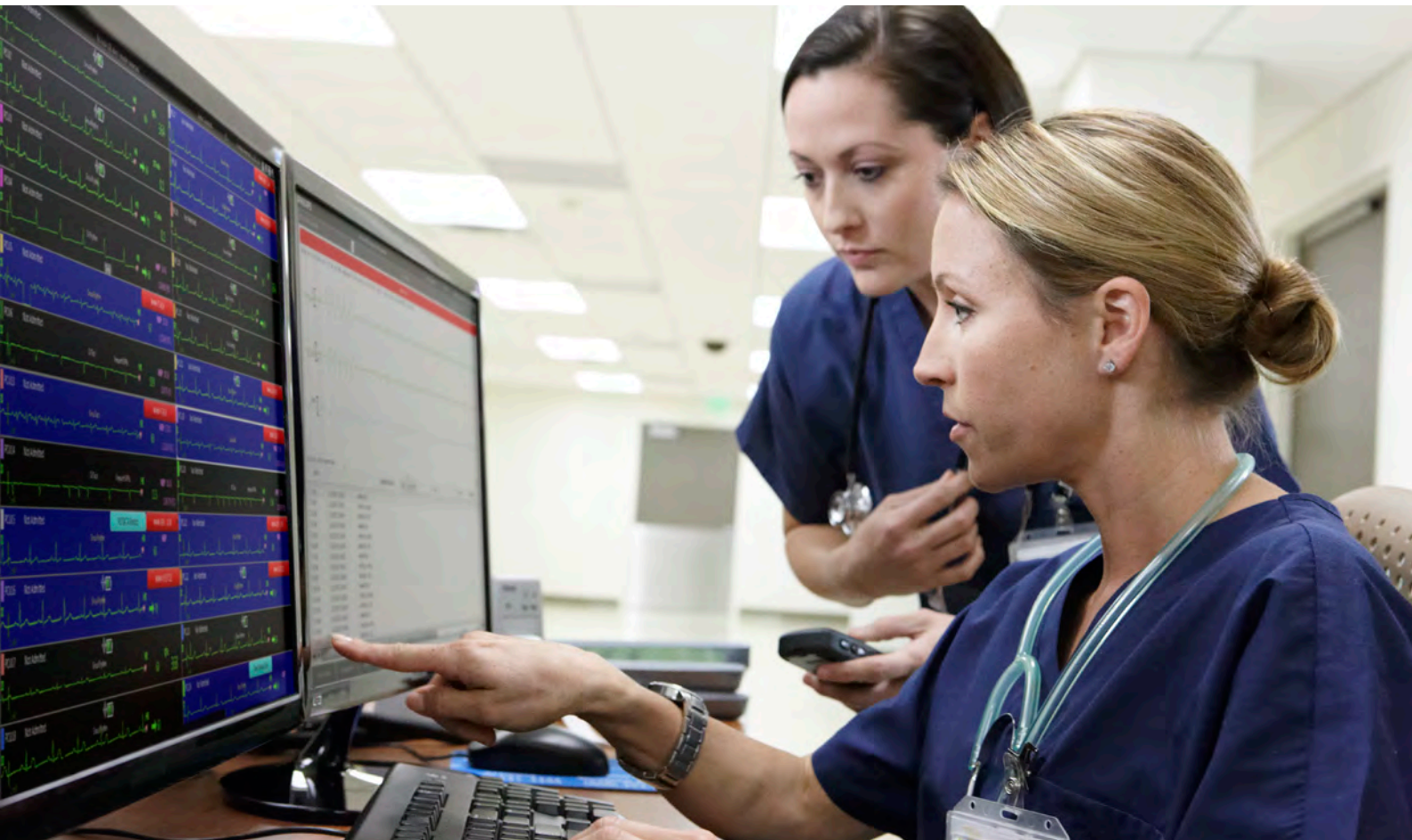


Figure 2: Patient monitoring reference architecture.



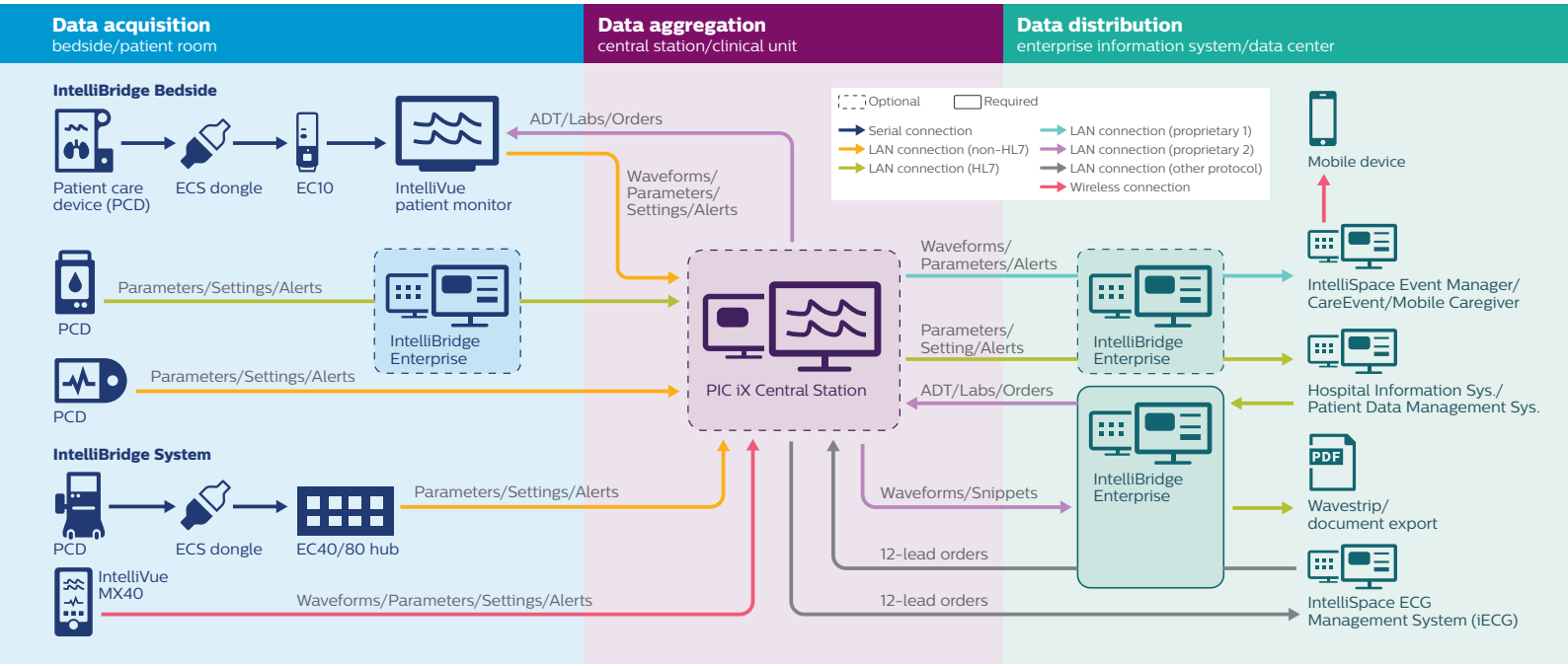
Knowing the patient monitoring ecosystem is key to understanding healthcare cybersecurity

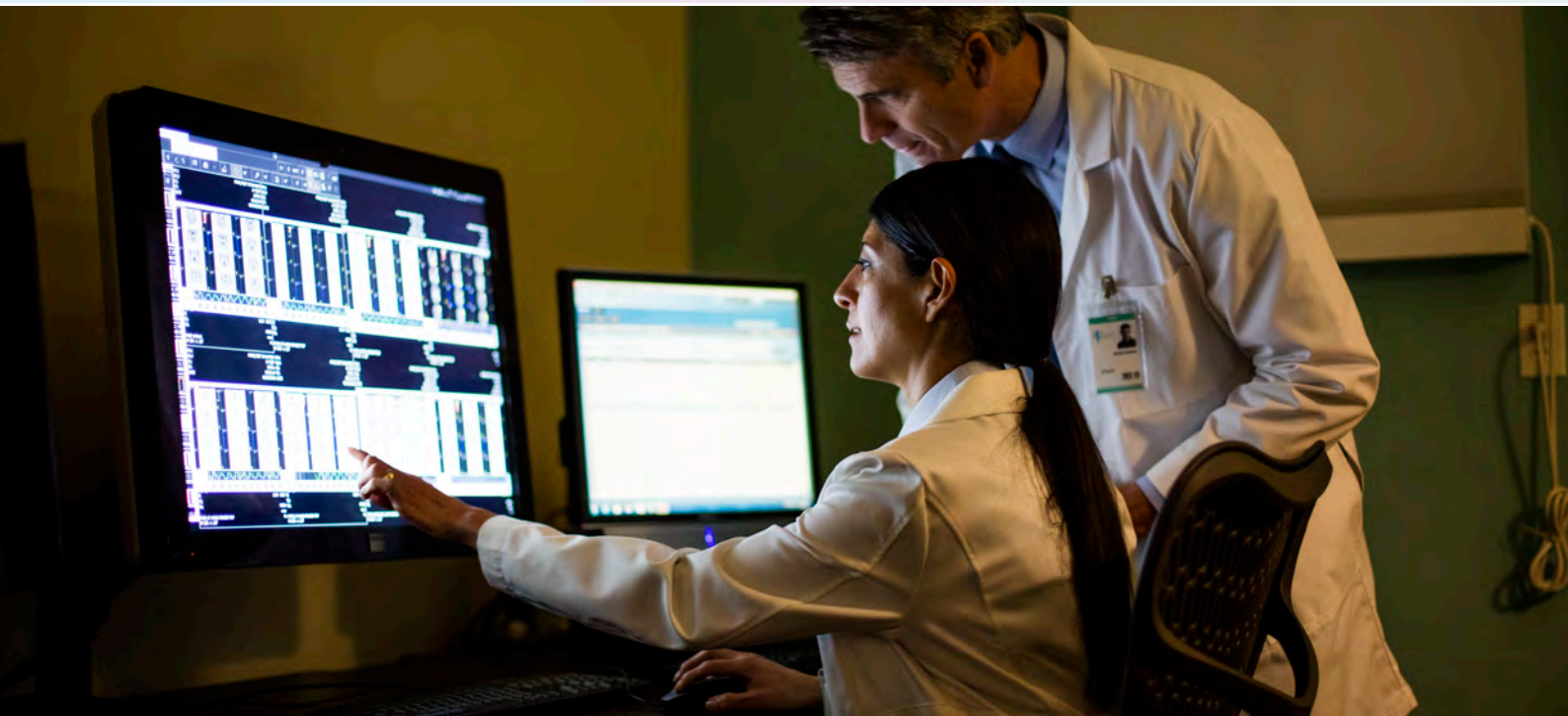
The IntelliVue Patient Monitoring Solution is a complex ecosystem of interconnected devices that provide life-critical information in real-time; that must continuously operate 24 hours a day, seven days a week, 365 days a year. Life-critical information includes patient vital sign data acquired from the patient and aggregated from multiple sources, resulting in the distribution of waveforms, trends, alarms and numerics to multiple systems including the Electronic Medical Record (EMR).

A multifaceted and holistic approach is essential to manage the ecosystem and maintain device manageability, serviceability, and security requirements.

Despite the fact that healthcare organizations are particularly vulnerable – and the majority of those surveyed in a 2017 Ponemon Institute study believed that they would be attacked within the next year – only 53% carried out any tests on their patient monitoring devices.[4]

Philips patient monitoring intended information flow diagram





Philips helps you overcome obstacles to secure your patient monitoring system

From security protocols and risk assessments, to a multi-layered offense and introducing the most innovative features, Philips follows best-in-class practices to provide you extra peace of mind.

Self-reporting

As a manufacturer of medical devices, one of the security protocols we're most serious about is self-reporting vulnerabilities. As a whole, Vulnerability Reporting – the practice of medical device manufacturers and independent researchers disclosing cybersecurity vulnerabilities – is up 400% more per quarter since the Food and Drug Administration released its cybersecurity guidance in 2016 according to a report by MedCrypt.[5]

That's good news for you. At Philips, we take ownership of security flaws and proactively report them, following this best practice process:

- Once a flaw is discovered, we report it to the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), a division of the Department of Homeland Security.
- It is then reported to the Food and Drug Administration (FDA).
- We are given an appropriate amount of time to fix the issue.
- We report the security flaw – and the resulting patch – to the public.
- We also proactively self-monitor on a weekly basis to stay on top of known issues and detect possible threats.

A multi-layered defense

There is no one single way to provide cybersecurity for your patient monitoring devices. That's why experts recommend an in-depth, multi-layer approach. Following best practices, each of these defensive layers plays an important role in helping obstruct hackers, defend against malware and prevent unauthorized access of medical devices. The layers include:

- Firewall
  - Operating System (OS) and Application hardening based on the US Department of Defense (DoD) Security Technical Implementation Guides (STIGs)
  - Authentication, authorization and accounting
- Audit Logging
- Encryption & node authentication

Philips defense-in-depth strategy

IEC 80001-1 best practices

This new international and voluntary standard outlines what you should focus on when connecting medical devices to your IT network in order to maintain safety, effectiveness and data and system security.

Although voluntary, we expect 80001-1 to become the healthcare norm. We recommend starting to apply the necessary policies and procedures to reduce the risks to medical IT networks.

The most innovative features

Bringing you the features you need when you need them is part of our commitment to helping you keep your hospital cyber-secure. Some of the features that set Philips apart from the competition include:

- Shipping Microsoft Windows 10
- Fully supporting validated OS security updates
- Integrating into your hospital domain
- Encryption
- SCCM

Looking forward and always trying to anticipate your needs

Technology moves fast. We stay one step ahead by continually innovating and introducing new features.

Together, we can maintain a secure environment by remaining vigilant and identifying the ever-changing cybersecurity threat landscape. We are committed to meeting your current and future needs.

More helpful resources

Department of Defense Vulnerability Disclosure Policy
https://hackerone.com/deptofdefense

Health Insurance Portability and Accountability Act (HIPAA)
Lists extensive requirements for privacy and security standards, including to the electronic transmission of health information. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

Application of Risk Management for IT-Networks Incorporating Medical Devices – Part 2-2 (IEC 80001-2-2)
Gives guidance for the disclosure and communication of medical device security needs, risks and controls. https://www.iso.org/standard/57939.html

Federal Information Processing Standard Publication 200 (FIPS PUB 200)
Provides a complete list of enterprise requirements. https://csrc.nist.gov/publications/detail/fips/200/final

National Institute of Standards and Technology 800-53 (NIST 800-53)
Outlines the security control baselines as the starting point for the security control selection process. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Sources

1. Becker's Health IT & CIO Report, 'The 3 most important security statistics healthcare organizations need to know', March 7, 2018, Mike Duffy; (https://www.beckershospitalreview.com/healthcare-information-technology/the-3-most-important-security-statistics-healthcare-organizations-need-to-know.html).
2. Reuters, 'Your medical record is worth more to hackers than your credit card', September 24, 2014, Caroline Humer, Jim Finkle; (https://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924).
3.-4. HIT Consultant, 'Protecting Medical Device Security in the Age of Ransomware', June 25, 2018, Kayla Matthews; (https://hitconsultant.net/2018/06/25/medical-device-ransomeware/).
5. Healthcare IT News, 'Is FDA doing enough to support medical device security?', August 15, 2018, Jessica Davis; (https://www.healthcareitnews.com/news/fda-doing-enough-support-medical-device-security).

Additional resources used:
Biomedical Instrumentation & Technology, 'The Vital Role of Device Manufacturers as Cybercitizens', November/December 2015, William L. Holden; (http://www.aami-bit.org/doi/abs/10.2345/0899-8205-49.6.410).

For more on Philips IntelliVue Patient Monitoring Solution, please visit **www.philips.com/monitoring**.

© 2019 Koninklijke Philips N.V. All rights reserved.

4522 991 51571 * JUL 2019

www.philips.com