Cyberattacks: the invisible threat to patient safety

The digitization of healthcare has given caregivers the power to access, analyze, manage and share patient data, helping to transform care and lower costs. But millions of connected medical devices, systems and networks make hospital and patient data highly vulnerable to cybercrime.

Hospital data under attack

Ransomware and hacking are the primary cyber-threats in healthcare,[1] and news about attacks aimed to disrupt clinical operations are continually in the news for disrupting health care and billing information operations.

Over the past five years, there has been a **256%** **increase in large breaches** reported to the U.S. Department of Health and Human Services involving hacking and a **264%** **increase in ransomware.**[1]

These threats, typically in the form of ransomware attacks, ultimately represent a serious disruption to the mission of providing quality healthcare to patients. This disruption is getting even more complex and resource-intensive as hospitals struggle to meet existing stringent security regulations. In the United States, hospitals strive to meet software bill of materials (SBOM) standards. Hospital leaders face similar pressure in the European Union as they prepare to meet the mandatory the NIS 2 cybersecurity directive deadline this Fall. The threats are significant enough in the United States to warrant proposed cyber legislation[2] that would

allow providers to receive advance payments in the event of a cyber incident, provided they meet minimum cybersecurity standards. This would provide more incentive – but more pressure – to increase cybersecurity measures.

Ensuring compliance with legislation has never been more important – or more timely.

Connected but not protected

While the healthcare IT industry is becoming a lucrative target for malicious activity, more and more medical devices are connecting to hospital networks, feeding EMR systems with physiological data. The multitude of vendors, legacy networks and devices in any given hospital provides attractive access points for bad actors to extract volumes of valuable patient data. And data that's been compromised is data that's not available for clinicians to use to make timely decisions at the point of care.

This points to a critical aspect of cybersecurity: protecting data availability. If data isn't available or reliable, clinicians don't have the insights they need for decision-making at the point of care, this can affect care quality and patient safety. And security gaps, ranging from a lack of maintenance of existing infrastructure, or the use of unsupported legacy systems, put hospitals and their patients at risk.

Hospitals are healing environments, not cybersecurity firms

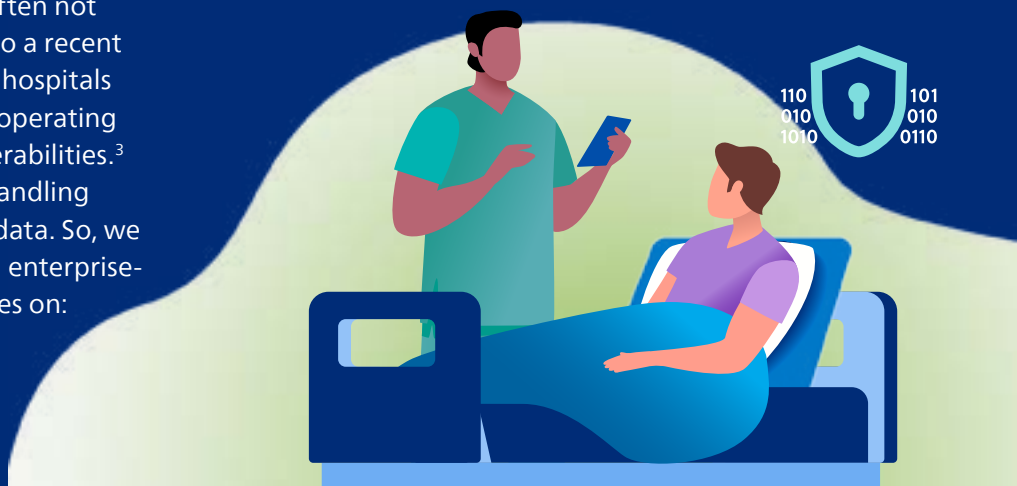
With increased threats to patient safety and business continuity, healthcare leaders must advance security measures to protect data confidentiality, integrity and availability. They must go from protecting network data and preventing downtime of compromised devices to implementing a more secure enterprise-wide strategy.

Yet hospitals and health systems are often not equipped to do this alone. According to a recent study, 95% of medium and large sized hospitals say they're operating with end-of-life operating systems or software with known vulnerabilities.[3] We recognize that our technology is handling increasing amounts of health-related data. So, we embrace a partnership approach to an enterprise-wide cybersecurity solution that focuses on:

Confidentiality
Only those who should have access can retrieve data.

Integrity
Information can't be modified without detection.

Availability
Information can be accessed when needed.



Staying one step ahead with an end-to-end cybersecurity strategy

Philips is well-equipped to help hospital IT and BioMed teams meet cybersecurity challenges and we have a history of doing so. We're committed to deploying secure hospital patient monitoring systems at installation, while helping hospital teams post-installation to develop a comprehensive security strategy that ensures the safety of products, business (enterprise information) and personal (patient) data.

We use a multi-layered, security design approach that encompasses everything from initial software coding, vulnerability testing, release and deployment, compliance with regulatory entities to ongoing threat management. This can help:

- Protect data from unauthorized access and increase data and system availability
- Understand how embedded security controls within devices are effectively enabled
- Recover quickly from interruptions while still protecting patient data

Philips healthcare IT services can help you develop a comprehensive cybersecurity strategy, from 24/7 monitoring with OS patching and antivirus response to implementing informatics service agreements, which include software upgrades and related clinical training, a patient monitoring security assessment and interoperability consulting, so you stay current and secure.

- Ease ongoing management and maintenance for IT with centralized access
- Diagnose and fix security technical issues remotely to speed resolution

With an enterprise approach to patient monitoring, cybersecurity is simplified by using a centrally managed system. This can ease ongoing management and maintenance, including using systems such as Philips Focal Point to help diagnose and fix security technical issues remotely to speed problem resolution. At Philips, we keep advancing our security measures, services and systems to proactively address concerns and alleviate some of the burden from IT and BioMed resources.

Keeping hospitals focused on healthcare means always staying one-step ahead – steps that Philips takes daily on behalf of our hospital partners and will continue to as long as there's a threat. **At Philips, network health equals patient health.**

References

1 Affairs (ASPA) AS for P. HHS Office for Civil Rights Issues Letter and Opens Investigation of Change Healthcare Cyberattack. www.hhs.gov. Published March 13, 2024. https://www.hhs.gov/about/news/2024/03/13/hhs-office-civil-rights-issues-letter-opens-investigation-change-healthcare-cyberattack.html

2 18TH CONGRESS 2D SESSION. Accessed October 11, 2024. https://www.govinfo.gov/content/pkg/BILLS-118s4054is/pdf/BILLS-118s4054is.pdf

3 HHS 405(d). Hhs.gov. Published 2024. https://405d.hhs.gov/Documents/405d-hospital-resiliency-analysis.pdf

www.philips.com