CYBERSECURITY IN THE CONNECTED HOSPITAL

New white paper shares perceptions of medical device cybersecurity, need for collaboration to address cyber challenges.

In today's digital world, the rise of connected health – advanced, technology-enabled tools that provide people and their physicians with information to better manage their health – is transforming patient care. Studies have shown that connected devices can significantly improve patient outcomes by reducing hospitalizations and the overall cost of care.[1]

Of course, as with any other internet-enabled technology, enhancing connectivity for medical devices also requires a strengthened focus on cybersecurity. The same powerful technology that multiplies the value of medical devices and data can also present risk to connected healthcare's integrity and availability if not managed and understood effectively by all stakeholders within the connected environment.

To better understand the perceptions and awareness of medical device cybersecurity, Abbott and Brunswick Insights surveyed 300 physicians and hospital administrators to learn about the cyber challenges they face in the hospital environment. Survey findings were recently released in a white paper co-authored by Abbott and The Chertoff Group, a security and risk management advisory firm.

Key findings include:

- Cybersecurity is a priority in the connected hospital: 92% of physicians and 91% of hospital administrators say that keeping patient and hospital data secure is a focus of their hospital.
- Physicians and hospital administrators feel underprepared to combat cyber risks: 75% of physicians and 62% of hospital administrators feel inadequately trained or prepared to mitigate cyber risks that may impact their hospital.
- Physicians and hospital administrators view medical device cybersecurity as a shared responsibility: 71% of physicians and 74% of hospital administrators believe cybersecurity is a shared responsibility among all participants in the healthcare system.
- Communication about medical device cyber-related vulnerabilities can improve: Only 15% of physicians and 45% of administrators report having seen or read advisories related to medical device security in the last six months.
- Standards are widely desired: 82% of physicians and 73% of administrators believe there should be industry-wide standards and consistent terminology.

Using these survey insights, Abbott and The Chertoff Group included in the white paper key considerations and ways the connected healthcare ecosystem must come together to address the cyber risks that face the entire healthcare industry, including:

- Industry-wide standards and cybersecurity by design to ensure cybersecurity protections are built into medical device development and that physicians and patients feel confident in the security and safety of the devices they use.
- Investment in cybersecurity incident response processes for identifying and responding to vulnerabilities in a timely manner, while supporting safe clinical care.
- Improved education, focus and training to increase all stakeholders' understanding of cyber risk in the healthcare setting.

To learn more details about the survey findings and what comes next, check out the press release and infographic about cybersecurity in the connected hospital.

References

1. Slotwiner D, Varma N, Akar JG, et al.: HRS Expert Consensus Statement on Remote Interrogation and Monitoring for Cardiovascular Electronic Implantable Devices. Heart Rhythm 2015; 12:e69–e100