When a nationally-recognized health system conducted an internal audit that uncovered gaps in medical device security practices, administrative leaders knew a change was in order. The current cybersecurity threat climate demands vigilance to protect healthcare institutions, their employees, and the patient community. Seeking urgent help and an experienced partner, the health system turned to Burwood Group to develop a cross-departmental security risk management program to proactively prevent and protect against cyberattacks.


To evaluate the security of its medical devices, the health system performed an internal audit and discovered the need for requisite cybersecurity processes and IT controls to fully secure its devices and patient data from breaches and cyberattacks. The health system's limited asset management system contained devices that could not be secured because they were based on obsolete operating systems. In addition to process and system limitations, the clinical engineering and technology teams were seeking ways better collaborate across departments.

The health system had already trusted Burwood Group to spearhead several initiatives, including its connected care governance program and IT activation and transition of a new outpatient pavilion. Burwood’s healthcare security practice team was a natural fit to develop and implement a medical device cybersecurity assessment and risk management strategy.

Client Success Story

Academic Health System Launches Cybersecurity Program to Safeguard Medical Devices and Patient Information

When a nationally-recognized health system conducted an internal audit that uncovered gaps in medical device security practices, administrative leaders knew a change was in order. The current cybersecurity threat climate demands vigilance to protect healthcare institutions, their employees, and the patient community. Seeking urgent help and an experienced partner, the health system turned to Burwood Group to develop a cross-departmental security risk management program to proactively prevent and protect against cyberattacks.


To evaluate the security of its medical devices, the health system performed an internal audit and discovered the need for requisite cybersecurity processes and IT controls to fully secure its devices and patient data from breaches and cyberattacks. The health system’s limited asset management system contained devices that could not be secured because they were based on obsolete operating systems. In addition to process and system limitations, the clinical engineering and technology teams were seeking ways better collaborate across departments.

The health system had already trusted Burwood Group to spearhead several initiatives, including its connected care governance program and IT activation and transition of a new outpatient pavilion. Burwood’s healthcare security practice team was a natural fit to develop and implement a medical device cybersecurity assessment and risk management strategy.

"Facing today’s threat climate, we needed a trusted advisor to step in and develop a cybersecurity program that would protect our staff and patients. We knew we could rely on Burwood Group’s deep understanding of the security vulnerabilities impacting the healthcare industry. Their solution has empowered our organization to proactively manage our security environment and has fostered a greater sense of ownership and interdepartmental collaboration across our health system.”

- Chief Information Officer

Burwood Group Services
- Technology Strategy
- Network Security
- Clinical and Operational Subject Matter Expertise
- Project Leadership
- Program Management
The Solution: Multi-Phased Cybersecurity Assessment and Risk Management Strategy

To evaluate existing and future vulnerabilities threatening the health system’s IT infrastructure, data security, confidentiality, and integrity, Burwood Group conducted a risk assessment on a sample of medical devices – for example, those containing ePHI risk and those requiring network connectivity. The team utilized a risk model to identify devices to be deemed “high-risk.” The team utilized MDS2, an industry-standard form that allows device manufacturers to provide security information to healthcare providers regarding their devices. While the form is an excellent tool for capturing information, it does not allow healthcare providers to perform a risk assessment based on the information provided. Thus, Burwood Group enhanced the form to accommodate risk scoring as well as the ability to obtain a final risk score, providing the health system’s clinical engineering and IT teams a way to efficiently evaluate the risks posed by devices entering their environment.

Burwood Group’s vulnerability management plan included research and configuration of the selected medical devices, enabling the health system’s clinical engineering staff to maintain and assess the security of the devices going forward. In the remediation phase, Burwood consultants implemented the vulnerability management plan based on the high-risk findings and analyzed the health system’s asset database to ensure it was functional for managing the security of devices well into the future. Current roles and responsibilities across hospital departments related to medical devices were also identified and better defined. Security policies and procedures were updated to reflect these updates.

Medical Device Cybersecurity Program Components:

- Asset Management
- Device Risk Management
- Vulnerability Management
- Security Hardening & Monitoring
- Incident Response

The Outcome: Medical Device Security Program Governance and Cross-Departmental Alignment

Today, the academic health system is equipped with a multi-year cybersecurity program that allows it to identify and protect its medical devices, detect incidents, respond with a plan, and recover normal operations. An integrated procurement process now enables the health system’s IT department and clinical engineering team to practice vigilance and better evaluate or disqualify medical device vendors that are not in compliance of the critical components of the health system’s new security program. Its updated asset management capability allows the health system to better control risks to medical devices with enhanced tracking and continuous oversight for ensuring secure and effective devices for its patients and staff.

Today, the health system’s Clinical Engineering, IT Security, and other related departments now adhere to a medical device security program governance model, as well as a set of well-defined roles and responsibilities. This roadmap has helped the health system to bridge operational gaps that leave them vulnerable to cybersecurity threats, and foster greater collaboration across the institution.

About Burwood Group

Founded in 1997 and headquartered in Chicago, Illinois, Burwood Group is a healthcare technology consulting firm that helps local, national, and international organizations bridge business strategy and technology solutions. During the past 20 years, Burwood Group has worked with over 170 healthcare organizations. Our clients choose Burwood Group to ensure their technology decisions and integrations improve the delivery of patient care. Learn more about our team at www.burwood.com/healthcare.