Increasingly, medical devices, including bedside patient monitors, infusion pumps, ventilators, and imaging systems, are being connected to and reliant on the hospital network. That connectivity brings the risk of intrusion by cybercriminals, who could steal electronic patient health information (PHI), install malware, alter treatment delivered by the equipment, or render the equipment unusable.

In July 2014, the Clinical Engineering Support Services (CESS) department of Intermountain Healthcare determined through an internal audit that, like many large hospital systems, a sizable portion of its medical equipment was at risk of cyberattack. With an integrated delivery network (IDN) spanning 23 hospitals and more than 285 clinics throughout Utah, southern Idaho, and northern Nevada, Intermountain poses a tempting target for those looking to steal sensitive data.

In July 2014, the Clinical Engineering Support Services (CESS) department of Intermountain Healthcare determined through an internal audit that, like many large hospital systems, a sizable portion of its medical equipment was at risk of cyberattack. With an integrated delivery network (IDN) spanning 23 hospitals and more than 285 clinics throughout Utah, southern Idaho, and northern Nevada, Intermountain poses a tempting target for those looking to steal sensitive data.

The professionals charged with defending Intermountain’s network faced a monumental task. CESS supports approximately 101,000 pieces of medical equipment, with more than 15% connected to the hospital network. Leadership from the CESS and the Information Technology (IT) departments determined that clinical and technical staff would need to compile data describing the risk, impact, and safety of patient care for all of that network-connected medical equipment.

“We needed to comprehensively understand what medical equipment we had throughout our system that stored, displayed, or transmitted any type of electronic PHI,” said Mike Busdicker, a system director for CESS at Intermountain Healthcare. “We want patients to feel as comfortable as possible knowing that we’ve got their safety in mind first, that they receive the best care and treatment possible. Ensuring that their personal health information is protected is a big part of that.”

But with so many devices to evaluate, the first and perhaps biggest step was determining which ones posed the greatest risk—and ultimately, where to allocate limited resources.

To defend patients from cyberattacks, the IT and CESS departments at Intermountain would need to develop a plan—and a program—to systematically review network-connected medical equipment.
tain Healthcare,” said Priyanka Upendra, compliance manager for CESS. Staying compliant with the HIPAA Security Rule and addressing all socio-economic aspects to protect electronic PHI kicked off this effort. Industry standards supplement our risk assessment and remediation efforts.”

**Challenge**

Intermountain’s CESS team was concerned with two issues: directly protecting patient safety from hackers and safeguarding their sensitive data.

“The biggest issue on our mind right now is—how do we make sure that medical equipment providing direct patient care doesn’t cause harm to the patient in case of a cyberattack?” said Shawn Anderson, information systems security analyst with Intermountain’s IT Cybersecurity Architecture team. “Then, we scale back on the risk. If it’s not going to affect patient safety, what are the biggest risks? That could be using the equipment to access the rest of our network.”

To ensure that Intermountain maintained compliance with federal regulations, staff needed to pore through Intermountain’s large equipment inventory to evaluate how patient data are used and assess their vulnerability to cyberattack. As staff reviewed the equipment, they had to ask several questions relating to how PHI is used: Does the equipment display, transmit, or store PHI? If it only displays PHI, then CESS would classify it as a “low-risk” system. Equipment that stores or transmits PHI is considered higher risk, and requires more in-depth analysis.

“In that case, we have to ask questions like: ‘What do we have that contains patient records?’ ‘How much does it store?’ ‘Is the storage temporary or permanent?’ Busdicker said. “After that, we start taking a look at Manufacturer Disclosure Statement for Medical Device Security (MDS2) information and incorporate that into our scoring methodology. It’s this whole process that led us to develop an internal application.”

Early on, the CESS team ran into a roadblock—some manufacturers were reluctant to provide documentation that detailed the cybersecurity vulnerabilities inherent in their various medical equipment models. That included MDS2, operator and service manuals, system architecture, patching and upgrade policies, and PHI disposal methodologies. All of that information must be collected and processed manually.

Intermountain staff were taken aback at this resistance, because they were seeking the information for their own defenses and to share with partner organizations.

“There’s a lot of concern from manufacturers that this is all proprietary information. That by exposing these weaknesses to other parties, we would be increasing the potential security risks for these devices,” Anderson said. “It was a little surprising to me that that mentality still exists with some suppliers—that ‘as long as we keep our vulnerability as a secret, we’re all safe.’ That’s just not the cyberworld that we live in anymore.”

The relationship between a healthcare system and the medical equipment manufacturers should be built on a foundation of trust, Upendra said, and having those technical details allows professionals in a hospital system to improve patient care. Fortunately, the resistance to share information did not extend to all manufacturers, and a sustained effort led many to get on board with the project.

“Over the last few months, we have called, emailed, and met with our suppliers to...
Intermountain Healthcare referenced the following reports for the project:

- Food and Drug Administration (FDA). Guidance for Industry, FDA Reviewers, and Compliance on Off-The-Shelf Software Use in Medical Devices
- FDA. Guidance for Industry - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software
- FDA. Infusion Pumps Total Product Life Cycle Guidance for Industry and FDA Staff
- FDA. Postmarket Management of Cybersecurity in Medical Devices Guidance for Industry and Food and Drug Administration Staff
- AAMI TIR 57/Ed. 1, Principles for medical device security—Risk management
- NIST 800-53 Rev 4, Security Controls and Assessment Procedures for Federal Information Systems and Organizations
- NIST Cybersecurity Framework

update them on Intermountain’s network security and CESS policies. We have had remarkable responses so far,” Upendra said.

Efforts are in progress to review medical equipment contracts to include data security elements and update the computerized maintenance management system (CMMS) with end-of-life and end-of-support notices from original equipment manufacturers.

Solution

Intermountain staff faced the daunting task of identifying and evaluating cybersecurity risks for thousands of pieces of medical equipment. They needed a way to systematically sift through the data and determine where to prioritize limited resources. In response to this challenge, two teams within Intermountain’s IT department (Cybersecurity Architecture and Application Development) worked with CESS to develop a computer application called Polestar.

Polestar, which is still in development, is designed to assess and rank the equipment’s PHI data using predefined criteria. Staff must manually enter information expanded from the MDS², supply chain, compliance, and other sources into the Polestar risk assessment. The program then automatically calculates a risk rating based on weighted factors, such as patient safety impact, likelihood of occurrence, and risk mitigation capability.

“The residual risk for each equipment model takes into account the risk and mitigation factor for each question in the assessment. There are efforts in progress to refine this algorithm to include a comprehen-

Figure 1. Device profile in Polestar
sive set of questions from supply chain, compliance, and legal, and patient safety teams,” Upendra said.

Based on that rating, along with information on clinical workflows and the equipment’s technical capabilities, a risk mitigation strategy is designed and proposed with Intermountain’s clinical and technical experts (Figure 1).

“As you answer each question in the Polestar application, an algorithm computes a final score and classifies devices as high, medium, or low risk within the system,” Busdicker said. “We didn't go out and reinvent the wheel on a lot of this. We weighted information from the MDS² sheets supplied by the manufacturers. We also developed some of our own patient safety and risk questions.”

Some answers will immediately earn a “critical” classification in Polestar. A “critical” device would be one where there's significant risk of patient harm associated with a cybersecurity compromise or if more than 500 patient records could be affected. For example, a cyberincident could alter drug delivery dosage rates or render the equipment unusable, causing harm or, in certain cases, death to a patient (Figure 2).

Critical risk factors outlined in the Polestar cybersecurity risk assessment are:

- Data stored or managed offshore.
- Equipment was identified as a cyberhack risk by verified sources.
- Loss of 500 or more local protected data records.
- Change or discontinue medication dosage.
- Compromise or render the device unusable.
- Change or destroy local biometric data.
- Interrupt life-sustaining medical services.

Polestar also interfaces with Intermountain’s CMMS, with information flowing in both directions. Medical equipment model information from the CMMS is fed into the program, and the protected data disclosure statement identification and residual risk rating are then sent back to the CMMS. Discussions are in progress to automate the identification of network-connected medical equipment and include their IT profile information in the CMMS, though Upendra said there are concerns about disrupting clinical workflow.

Overall, Polestar helps prioritize work to catch the lowest-hanging fruit as well as the most important cybersecurity items. If the program classifies a device as “low” or “medium” residual risk, then the Cybersecurity Architecture team’s direct involvement is bypassed, and a facility-specific CESS team will work with medical equipment manufacturers to mitigate risks. The risks associated with these categories are evaluated with clinical, legal, compliance, and other business groups to develop an effective mitigation plan.

“If it comes up as ‘high’ or a ‘critical,’ that’s when Cybersecurity Architecture is re-engaged in the process. We might do additional development of security-compensating controls or some other types of isolation. Or maybe we make recommen-

![Figure 2](https://example.com/polestar_2.png)
Polestar’s risk assessment is then followed up with a plan that brings all the stakeholders to the table. From that plan, the IT and CESS teams work along with clinicians and device manufacturers to develop a fix. That could include implementing new device features, testing for encryption, or isolating the device on the network—particularly legacy devices that are too old to receive an upgrade (Figure 3).

“On the cybersecurity side, we focused really heavily on the network isolation component, especially since for a lot of the devices, we can’t do anything with them from security mitigation standpoint,” Anderson said. “If we can develop the proper network isolation, the ability for it to affect the rest of the network or other devices on the network is limited.”

Next Steps

The integration of Polestar at Intermountain is still ongoing, but the project poses several potential benefits for CESS and the IDN as a whole, including:

- Identification of all network-connected equipment (i.e., medical equipment, clinical support systems, facility utility systems).
- Systematic cybersecurity risk assessment process.
- Information sharing across all Intermountain facilities (clinical and business groups).
- Information gathering and IT profiling.
- Bidirectional communication with Intermountain’s CMMS.

The Intermountain team is also engaging in training programs to drive home the importance of cybersecurity for clinicians and the executive leadership, who may not be fully aware of the risks. Medical equipment cybersecurity is a critical part of Intermountain’s 2017 compliance work plan, Upendra said. Over the next year, Intermountain will perform a mandatory cybersecurity review when evaluating and procuring medical devices. The CESS team plans to gather information and perform cybersecurity risk assessments for a quarter of Intermountain’s high-risk medical equipment (about 860 unique models), sanitize PHI and other sensitive information when disposing of medical equipment, and create mandatory computer-based training modules to make employees aware of cybersecurity risks.

“Over the next 2 years, CESS will work actively with patient safety committees,
compliance, legal, clinical, and technical experts across Intermountain Healthcare facilities to build a strong foundation to the medical equipment cybersecurity program,” Upendra said. “This will include the cybersecurity piece in our staff education programs and throughout the life cycle of medical equipment at a healthcare delivery organization.”

The hope is that the processes and information gained can be shared throughout the industry, Upendra said. The Intermountain team demonstrated Polestar for the first time at the National Health Information Sharing and Analysis Center fall summit in San Diego, CA, in November 2016, where the program drew interest from manufacturers and other healthcare organizations.

“It’s up to us to get out there and educate across the industry on what the risk is when it comes to cybersecurity and patient safety. This is a huge educational opportunity,” Busdicker said.

The team is working with the Medical Device Innovation, Safety and Security Consortium, Medical Device Security Information Sharing Council, Provider Security Information Council, and experts at the Food and Drug Administration, and AAMI to develop medical equipment security programs, share information, and develop a framework that other healthcare delivery organizations can draw from.

“Our ultimate goal is to help drive processes and workflows around medical equipment cybersecurity that mitigate risk across the healthcare industry as a whole,” Upendra said. “This approach has helped us be more proactive than reactive, for us to understand the cyberrisks within this ecosystem and also to manage them.”

The Intermountain team demonstrated Polestar for the first time at the National Health Information Sharing and Analysis Center fall summit ... where the program drew interest from manufacturers and other healthcare organizations.

---

**A Practicum for Healthcare Technology Management**

This revised textbook is the go to resource for new and seasoned biomedical professionals. It covers everything from The Joint Commission accreditation process and managing medical device safety to human factors engineering and evidence-based medical equipment maintenance management.

**Based on Les Atles’ best-selling title and written by experts in the profession.**

**Order Code:** BETM2 or BETM2-PDF

**Order Your Copy Today!**
**Call 877-249-8226 or visit www.aami.org/store**