INSIDE THE INFUSION THERAPY DEVICE SECTOR


Matthew Hutchings


Rob Suárez


Alyssa Moy

Infusion therapy devices have been in the news lately—due, in no small part, to concerns surrounding their hackability. Below, two individuals representing the infusion therapy manufacturing sector—Rob Suárez, vice president, chief information security officer at BD, and Matthew Hutchings, ICU Medical's vice president, global marketing and innovation, infusion systems—join Alyssa Moy, director, adoption and integration at home and alternate treatment site infusion therapy services provider Option Care, to discuss what's new in infusion therapy and how HTM professionals are integral in keeping infusion devices secure. Don't miss out.

24x7 Magazine: What are the top trends in the infusion therapy sector, and how are they influencing the design of such technologies?

Matthew Hutchings: There are really four key categories driving the course of innovation in infusion therapy at ICU Medical: First, there's the growing importance of IV-EHR interoperability, or the connecting of smart pumps to enterprise-grade electronic health record systems and other third-party applications to help increase clinician and patient safety, enhance workflow experiences, and improve device management within the health system.

With the increase in connectivity among systems comes the second driving factor for us, which is cybersecurity and ensuring that our devices and corresponding safety software are as safe and secure as possible. Also, with greater access to a wider range of clinical and business data comes the need to provide meaningful business analytics; more near real-time infusion data; and dash-boarding for medication management and accurate billing to turn this wealth of data into usable, actionable information that can drive clinical and business decision-making. And, finally, all this is taking place in an environment where hospitals are demanding products and systems that deliver clinical and economic value at the overall lowest total cost of ownership.

Rob Suárez: From a cybersecurity perspective, we are tasked with simplifying and reducing the interactions with medical technology when it comes to authenticating users. For example, this may mean adopting multifactor authentication to avoid cumbersome passwords. Also, there are advantages to wireless connectivity for infusion pumps for analytics and electronic medical record integration, which in turn require stronger security by design.

Alyssa Moy: Infusion therapy has its risks, and being able to monitor and report on a patient's clinical outcomes has influenced how we develop reporting capabilities and produce technology that interfaces with external providers to enhance a patient's results. Patients are not one-dimensional; they deserve a multi-disciplinary approach to care—and, through technology, we have the ability more than ever to monitor their therapy adherence, predict outcomes, and ultimately provide them with superior care.

24x7: How has the infusion therapy sector evolved in the past few years? How do you expect it to evolve even more in the future?

Moy: Three words come to mind: security, support, and accessibility. Now more than ever, patients are concerned about the security of their information—particularly when it comes to the electronic medical record. We're doing our best to create a 'security culture' and adopt core preventive security measures, which are sought after and appreciated by our current and prospective patients. Patients also expect a certain level of ongoing support throughout the duration of their therapy.

A chronic illness no longer means limited mobility or reduced quality of life, thanks to the help of technology—which allows patients and caregivers to manage their therapy electronically. Additionally, patients are willing to receive infusion therapy at 'alternate infusion sites' that are more retail-centric and provide amenities throughout the infusion experience. In the future, I expect patients and caregivers to further take charge and actively manage their treatment plans via mobile apps, artificial intelligence prediction tools, online payment plans, and the ability to tele-communicate with their nurses and care management providers on demand.

Suárez: At BD, for instance, we have made significant efforts [in recent years] to incorporate security throughout our quality management system, which includes design control, complaint handling and risk management. More companies are adopting vulnerability disclosure practices and improving transparency on the security issues that exist in medical technology. While we should still see more activity in coordinated vulnerability disclosures, this trend is

promising. In addition, there is more information that is publicly available to help medical technology companies improve security, such as the Medical Device and Health IT Joint Security Plan.

Hutchings: Thankfully, infusion therapy has evolved from a time where every element of the IV system was viewed in isolation and seen as a standalone device. The infusion pump advanced to a "smart pump" that operated within a single hospital, to now being considered a key component that needs to operate within the context of a broader networked, enterprise-level healthcare organization's ecosystem.

Connectivity and clinically relevant enterprise-wide communication between the infusion pump, the drug library and medication management systems, and the EHR have moved to the forefront. As healthcare systems in the U.S. continue to converge, the demands for increased interoperability, consolidated enterprise-wide drug safety management, and analytics will be drivers of existing product enhancements and innovation in the future.

24x7: Infusion therapy devices have made headlines recently for their susceptibility to hacking. How is your company addressing cyber-concerns?

Hutchings: Given the fact that approximately 90% of patients admitted to U.S. hospitals receive IV therapy and that health systems may have thousands of IV pumps in their inventories, this is a critical risk case to address. ICU Medical has taken this very seriously. We are proud of the fact that we are the first medical device manufacturer to obtain certification under the UL Cybersecurity Assurance Program (UL CAP), a new cybersecurity management program from UL designed to minimize risks by creating standardized, testable criteria for assessing software vulnerabilities and weaknesses to help reduce exploitation, address known malware, enhance security controls, and expand security awareness.

We earned UL CAP certification for our Plum 360 drug infusion system that provides full interoperability with patient EHRs, reducing the need for manual input and transcription of infusion data to manage patient safety and clinician workflows better. We now have CAP certification for ICU Medical MedNet safety software, as well. While the UL 2900 standard was written with FDA pre- and post-market cybersecurity and American National Standards Institute technical panels guidelines in mind, we fully recognize that cybersecurity needs will continue to evolve—and our certifications and other cybersecurity measures are ongoing to help ensure security today and in the future.

Moy: Option Care uses a risk-based, layered approach to security. We focus on four pillars—governance, people, processes, and technology—to secure our environment within each of these layers, from outward- to inward-facing connections. This security includes third-party and other devices that connect with our network. People are our greatest assets and potentially our greatest risk. As a result, we developed an education and training campaign that takes place year-round and leverages "ambassadors," who are non-IT employees located around the country, to also spread the information security message throughout our locations and enterprise.

Suárez: We view cybersecurity as an ongoing process and all of our teams work in partnership with our customers, cybersecurity researchers, and regulators to ensure that we design secure products, identify present risks, and communicate with our customers in a timely manner about new risks as they are identified and how to mitigate them. While it may seem counterintuitive, as the defenders of technology and healthcare, our community needs to adopt a similar culture of information-sharing and make it open, free and transparent. In a coordinated and responsible way, companies can better match the pace at which new cybersecurity threats are emerging.

24x7: What do you want to tell HTM professionals about the handling and maintenance of infusion therapy devices and why?

Suárez: Securing medical technology requires partnership and collaboration. Our goal is to communicate security risks accurately and comprehensively, with readily available measures that customers can take to reduce or eliminate that specific risk. We want customers to understand why specific measures are selected and how they can help ensure products are secure by design, in use and through partnership, because you can't secure what you don't know. It is important to remember that all technology ages over time and vulnerabilities manifest; as we see more vulnerability disclosure, it is also a sign of greater transparency.

Hutchings: A significant historical concern around infusion therapy devices has been maintaining the device drug library safety software—the safety parameters managed by software updates on the infusion pump that limit over- and under-delivery of medication. These devices are now distributed across an enterprise versus a single hospital. Because of this, the historical challenges of locating devices to do preventative maintenance—in addition to applying upgrades, updates, and firmware patches to the devices themselves, along with applying medication safety updates for drug delivery limits—have been exacerbated. That's why we are providing customers with a real-time location system that includes a bidirectional connection to enable real-time visibility into their IV pumps' location and status, helping them save time while enhancing overall fleet operation.

24x7: What else do you want *24x7 Magazine* readers to know about the infusion therapy device sector?

Hutchings: Medical devices, and particularly infusion therapy pumps, have moved from a nursing, biomedical, and purchasing conversation to the forefront of healthcare IT. These devices have been rapidly increasing in complexity and sophistication—not only in their advanced level of required cybersecurity, but also in how they address the safe delivery of medications.

Moy: Market forecasts project CAGR growth of 5.6% within the next decade, with infusion pumps being the largest contributor to the global infusion devices market. Moreover, infusion pumps have recently become more interconnected through wireless networks and incorporate dose-error-reduction systems to increase patient safety. These devices open the door to interoperability with innumerable systems to further improve infusion safety, increase healthcare provider efficiency through automation of pump programming and documentation, and improve clinical decision-making by monitoring when infusions have discontinued and when changes are made to infusion rates. With this technological potential at our fingertips, healthcare providers should think about proactively budgeting for the future of 'intelligent' pumps versus 'smart' pumps to realize the benefits for both the provider and the patient. 1