Reliable and Scalable Infusion System Integration with the Electronic Medical Record

Daniel C. Pettus, Tim Vanderveen, Robert L. Canfield, and Robert Schad

Features

Editor’s note: This article is based on the authors’ combined 75 years of experience with configuring, deploying, and supporting intravenous infusion devices; their familiarity with wireless infusion products installed on complex hospital network environments; and the knowledge gained from achieving infusion system and electronic medical record interoperability at more than 165 hospitals to date. The approaches described here are presented to help educate and encourage further discussion; however, the authors acknowledge that other methods exist for achieving safe and reliable wireless connectivity and device integration.

In 2015, St. Vincent Healthcare in Billings, MT, received the American Society of Health-System Pharmacists Best Practice Award in Health-System Pharmacy for demonstrating the “Clinical and Financial Benefits of Smart Pump-Electronic Medical Record (EMR) Interoperability at a Regional Health-System Hospital.”1 St. Vincent, which is part of SCL Health System (headquartered in Denver, CO), documented the operational and patient safety benefits of implementing infusion system–EMR interoperability and the financial benefits of leveraging more precise charge-capture data to improve reimbursements.2

The industry has come a long way on this important journey, arriving at full, closed-loop interoperability. This article highlights the accomplishments of the journey by sharing the experience of one infusion system company as it transformed from being an equipment supplier to becoming an integral part of EMR meaningful use.

Any networked medical device must be reliable, scalable, and secure. Ensuring the security of any device is an ongoing process of anticipating and responding to developing threats. A meaningful discussion of the complexities of this process is outside the scope of this article. The focus here will be on technology and how the infusion system engineers needed to “think differently” to move beyond the barriers identified during development. Particular attention will be paid to a major turning point: namely, the company’s decision to scrap the original design after years of development. Real-world experience showed that more was needed to scale from hundreds of infusion devices on a single care unit to thousands of devices across entire hospitals or integrated delivery networks (IDNs).

The process of designing a new, infusion-specific, data-transmission protocol is described, in order to illustrate new ways of thinking required to develop one approach to achieving reliable, scalable, bidirectional communication. The success of these efforts is confirmed by current use of the resulting infusion system in EMR interoperability at more than 165 hospital sites and, most of all, by the clinical, operational, and financial results that have been achieved. What engineers envisioned years ago has become reality.

About the Authors

Daniel C. Pettus is vice president of IT and connectivity at BD/CareFusion in San Diego, CA. Email: dan.pettus@bd.com

Tim Vanderveen, PharmD, MS, was vice president of the Center for Safety and Clinical Excellence at BD/CareFusion in San Diego, CA. Email: tim.vanderveen@bd.com

Robert Canfield is an HIT specialist and senior product manager at BD/CareFusion in San Diego, CA. Email: robert.l.canfield@bd.com

Robert Schad is director of IT and connectivity at BD/CareFusion in San Diego, CA. Email: robert.schad@bd.com

About the Authors

Editor’s note: This article is based on the authors’ combined 75 years of experience with configuring, deploying, and supporting intravenous infusion devices; their familiarity with wireless infusion products installed on complex hospital network environments; and the knowledge gained from achieving infusion system and electronic medical record interoperability at more than 165 hospitals to date. The approaches described here are presented to help educate and encourage further discussion; however, the authors acknowledge that other methods exist for achieving safe and reliable wireless connectivity and device integration.

In 2015, St. Vincent Healthcare in Billings, MT, received the American Society of Health-System Pharmacists Best Practice Award in Health-System Pharmacy for demonstrating the “Clinical and Financial Benefits of Smart Pump-Electronic Medical Record (EMR) Interoperability at a Regional Health-System Hospital.”1 St. Vincent, which is part of SCL Health System (headquartered in Denver, CO), documented the operational and patient safety benefits of implementing infusion system–EMR interoperability and the financial benefits of leveraging more precise charge-capture data to improve reimbursements.2

The industry has come a long way on this important journey, arriving at full, closed-loop interoperability. This article highlights the accomplishments of the journey by sharing the experience of one infusion system company as it transformed from being an equipment supplier to becoming an integral part of EMR meaningful use.

Any networked medical device must be reliable, scalable, and secure. Ensuring the security of any device is an ongoing process of anticipating and responding to developing threats. A meaningful discussion of the complexities of this process is outside the scope of this article. The focus here will be on technology and how the infusion system engineers needed to “think differently” to move beyond the barriers identified during development. Particular attention will be paid to a major turning point: namely, the company’s decision to scrap the original design after years of development. Real-world experience showed that more was needed to scale from hundreds of infusion devices on a single care unit to thousands of devices across entire hospitals or integrated delivery networks (IDNs).

The process of designing a new, infusion-specific, data-transmission protocol is described, in order to illustrate new ways of thinking required to develop one approach to achieving reliable, scalable, bidirectional communication. The success of these efforts is confirmed by current use of the resulting infusion system in EMR interoperability at more than 165 hospital sites and, most of all, by the clinical, operational, and financial results that have been achieved. What engineers envisioned years ago has become reality.
**Closed-Loop, Infusion System–Electronic Medical Record (EMR) Interoperability**

- After a prescriber orders a drug, a pharmacist verifies the order to ensure appropriateness and sends it to the patient’s EMR.
- To administer an intravenous (IV) infusion, a nurse scans a patient’s armband to verify identity and the IV medication label to verify right medication, time, dose, and route, as shown on the order in the EMR.
- Scanning the barcode on the infusion device triggers wireless transmission of the ordered infusion parameters from the patient’s EMR to preprogram the device. The nurse verifies the information on the infusion device, accepts the data, and the infusion begins.
- Dose-error reduction software in the device protects against errors in any manual programming of titrations, bolus doses, STAT infusions, and infusions such as anesthesia and procedural sedation for which there would be no prescriber order.
- Time-stamped infusion data are wirelessly sent back to the patient’s EMR from the infusion device for the nurse to review and accept into the EMR.

**Interoperability**

Numerous studies have documented the need for infusion device–EMR integration. Among medication errors, those involving intravenous (IV) infusions have the greatest potential for patient harm. A single wrong keystroke in programming the device can result in a 10- or 100-fold overdose with possibly tragic results (“death by decimal”). In 2013, a query of the ECRI Institute Patient Safety Organization database showed that 75% of analyzed infusion programming errors could have been averted with successful infusion device–EMR integration. As a result of these and other reports, infusion device–EMR interoperability has become a major focus for improving patient safety and quality of care.

Such interoperability makes modern infusion systems unique among today’s medical devices. An integrated, closed-loop system both “listens” and “talks” to the devices. Although some patient monitors transmit and display data, interoperable infusion devices actually use and act on the data. Performing critical tasks—such as prepopulation of the device with the ordered infusion parameters from the EMR, automatic transmission of infusion data from the device to the EMR, and ongoing surveillance of infusion status, alarms, and alerts—requires reliable, scalable, bidirectional wireless communication among integrated devices.

The bidirectional communications path is highly complex, initiating from the EMR–barcode medication administration (BCMA) system, then going to the EMR infusion-programming application, the interface engine, the infusion server, over the hospital wireless network, and finally to the targeted infusion device, with end-to-end transmission occurring reliably in a matter of seconds (“near real time”) throughout the hospital or IDN. During infusion, time-stamped data from the device are sent to the EMR via the same path.

**The Journey Begins**

For one infusion device company, the journey to interoperability began in 1995 when its engineers had already envisioned the possibility of programming infusion devices automatically with infusion parameters transmitted from the electronic medical administration record. The company had a new type of “smart” (computerized) infusion device in program development, with dose-error reduction-software (DERS) designed to alert the nurse if device programming exceeded pre-established limits. The modularity of the system was designed to improve clinical workflow by standardizing the user interface for any infusion type. An additional benefit of the modular design was to reduce the number of messages and the wireless connections needed by combining data from multiple infusion sources into a single “infusion status update” to the server (Figure 1).

The engineers recognized that the fundamental architecture being developed also would need to support the bidirectional wireless communications that would be required for future autoprogramming. Several patents were filed describing what eventually would become bidirectional connectivity (master patent 5,781,442). The design considerations needed for such communications were added to the hundreds already being considered to bring the new
In addition to the smart infusion system, other technologies required further development before interoperability could be achieved. For example, although the BCMA systems introduced in the early 2000s could scan the IV medication bag, they did not communicate directly to the infusion device. Nurses had to manually program the infusion device. To move from error-prone manual programming to closed-loop interoperability, enhancements to the BCMA systems were needed to communicate with the infusion device and to associate the device with the patient. New EMR software was needed to send the ordered parameters to the infusion device.

By early 2002, the infusion device company was able to begin collaborating with a leading BCMA vendor to codevelop a system that would automatically program the device with the infusion parameters in the EMR and automatically document the infusion process. The resulting system was implemented in an intensive care unit (ICU) at Ohio Valley General Hospital in Pittsburgh, PA, and used in patient care from December 2003 to April 2004.¹³

A Major Turning Point
The 2003–04 implementation of infusion device–EMR interoperability was considered a success because it showed that the infusion device could be prepopulated from an EMR order electronically and reliably, thus reducing error-prone manual keystrokes. Time-stamped infusion data also could be sent to the EMR, improving the timeliness and accuracy of documentation.¹³

The system implemented at Ohio Valley General Hospital was designed to work with IEEE 802.11 wireless (Wi-Fi) technology, which was used by most hospitals at the time for networked laptops, tablets, and other devices. Over the years, various enhancements had enabled networks to better support mission-critical systems and devices found in healthcare environments, and commercial off-the-shelf (COTS) technologies were well supported by most network manufacturers. However, such protocols were developed primarily for web traffic, rather than specifi-
Features

Summary Design Considerations for Near-Real-Time Infusion Device Connectivity

- Bidirectional infusion-to-server communications must be reliable and efficient.
- Closed-loop, bidirectional, smart infusion device– electronic medication administration record communications must occur, end-to-end, as rapidly as possible.
- Connectivity messages will be event driven by autoprogramming, alarms, or changes in infusion status or programming.
- A common, single-server architecture must be able to support up to thousands of infusion channels from a common data center.
- Infusion device wireless connectivity must function reliably on a variety of hospital networks and operate within existing hospital requirements.
- Connectivity must consume minimal bandwidth on the hospital network.

- Remote locations (even hospitals hundreds of miles from the central server) must communicate with negligible degradation in performance.
- Raw infusion communication messages from the device must be secure and encrypted, as hospital wireless security and encryption cannot be guaranteed.
- Infusion devices must function reliably, despite any minor or major network disruptions.
- Connectivity messages will need to expand and scale over time to include the large-volume and syringe infusion and monitoring modules supported by the modular system.
- Connectivity messages will need to be continuous to support the persistent connection required by developments such as dashboards displaying multiple devices’ infusion status in near real time.

Initial Implementation of Infusion Device– Electronic Medical Record (EMR) Interoperability at Ohio Valley General Hospital: Lessons Learned

- Although commercial off-the-shelf (COTS) communication components worked well with a small number of infusion devices during development, their performance deteriorated as the numbers scaled during the initial implementation from 2003 to 2004.
- The infusion device developer could not control hospital Wi-Fi infrastructure or EMR latency times; instead, the company had to do everything possible to optimize what was under its control (i.e., the design of the infusion system and associated server applications).
- Relying entirely on COTS for end-to-end system design introduced variabilities and reduced the developer’s control over message and protocol optimization.
- The “one-to-many” communication schema between infusion devices and the infusion server needed to be targeted for custom development and optimization.
- The “one-to-one” communication schema between the infusion interface engine and the EMR should be based on existing standards like HL7 and later IHE Profiles (for reasons beyond the scope of this article).
- The infusion company needed to expand its implementation and support capabilities to help hospitals better manage the new interoperability workflow enhancements.
to recover lost connections). The new design replaced the COTS communication protocols at two layers.

**Device-to-Server Application Layer Messages**
The application layer was designed to provide packed, binary encoding of structured information. For example, if a status message had four possible state changes, then the encoded message would allocate two binary bits in the message payload. This significantly reduced message size from earlier design implementations. The binary raw messages contained in the application layer were designed exclusively for infusion device communication, thereby eliminating overhead from using COTS methods. An advanced encryption standard (AES) was used to ensure point-to-point encryption of the internal datagram packets. Using a unique, proprietary binary design also could make the raw messages more difficult to exploit.

**Device-to-Server Transport Layer Communications**
A standard transmission control protocol (TCP) connection transports datagrams and provides communication; however, the connection timeout and recovery in the TCP were not really designed for interactive use. When no data were being sent over the link, the TCP did not detect if the link was broken. Even when data were being sent on a TCP connection, it could take up to several minutes before TCP reported that a link was broken. To be able to respond to link failures more quickly and to detect a broken link even when a device was idle (i.e., not transporting application data), the engineers developed a unique, infusion device–specific transport layer protocol called device connection management protocol (DCMP). DCMP monitors the link and sends unidirectional “keep-alive” messages when the link has been idle for a predetermined (configurable) length of time.

**Figure 2.** Establishing and maintaining communication: typical secure sockets layer (SSL) “handshaking.” Workstations, tablets, and other user-centric systems use SSL handshaking and encryption to establish a connection with a resource. This requires the exchange of a series of messages, hand off of certificate files, and acknowledgment that the conversation is authorized. Handshaking must be done every time communication has to be renewed.
DCMP also allows a large number of networked devices to discover and maintain a secure connection with a centralized server, while still conserving bandwidth. A single 12-byte exchange is used to establish the initial connection between the device and the server and to send infusion data over the established connection. Whenever the device is idle, instead of allowing the connection to break and using handshaking to re-establish the connection (Figure 2), DCMP sends unidirectional, 5-byte keep-alive messages to maintain a persistent connection (Figure 3). Messages can be aperiodic (a change in status or autoprogramming events), or periodic (continuous feeds to a near-real-time status board display). DCMP is designed to handle both.

As reported in 2013, the minimal bandwidth utilization of the DCMP protocol has been validated through on-site testing at various hospitals and IDNs. Results show that even under peak transfer conditions, DCMP infusion pumps placed negligible load on the wireless data network. Hospital wireless environments continue to evolve, and on-site testing continues to be performed on a routine cadence. Results of these tests are monitored and evaluated to ensure that the infusion system's performance continues to meet the goals that were set for the design. However, meeting design goals is only one step on the road to on-site interoperability. Hospital environments vary widely, and the infusion system's performance on a given hospital's network is beyond the infusion-systems company's control. Data on bandwidth consumption, latency times, and other variables are helpful to confirm that design goals have been met, but ultimately there is only one test: Does the system work as needed in widely varying systems and networks found in today's hospitals and IDNs?
Clinical, Operational, and Financial Results

In 2012, Oklahoma Heart Hospital in Oklahoma City became the first hospital to integrate a modular smart infusion system using the DCMP protocol with an advanced EMR. That same year, EMR integration with the modular DCMP system also went live at the Minneapolis campus of Children’s Hospitals and Clinics of Minnesota and at the St. Paul campus the following year. By the end of 2013, an additional 75 hospitals had contracted for the implementation of closed-loop, infusion system–EMR interoperability using the infusion device company’s new system design.

Today, interoperability between the company’s infusion system and either of two different EMR vendors has been implemented in more than 165 hospital sites. As more hospitals contract for future implementation, the goals typically remain much the same as at St. Vincent: “to improve i.v. infusion medication safety; to improve the accuracy, timeliness, and efficiency of i.v. infusion documentation; and to increase revenue in outpatient areas through improved i.v. infusion documentation.”

A high level of collaboration by multidisciplinary teams, including pharmacy, nursing, quality assurance, clinical informatics, information technology (IT), healthcare technology management (HTM), project management, education, and EMR and infusion system vendors, was essential to successful implementation. The project kicked off in October 2013, and on May 13, 2014, interoperability between the EMR and infusion system was fully implemented on all care units, excluding the neonatal ICU and procedural areas (such as the operating room and catheterization laboratory).

Improved clinical and operational performance was evident in the documented results. Prepopulation of infusion parameters reduced the number of error-prone, manual-programming key strokes by 86%. Compliance in using interoperability to prepopulate the device was 70% to 80%. Monthly average DERS usage increased from 91.76% to 94.38% and patient identification usage from 35.54% to 80.96%. Average monthly decreases in infusion system alerts, alert overrides, reprogrammed infusions, and cancelled infusions were 22%, 20.5%, 19%, and 33%, respectively. Financial performance was improved by an almost 40% reduction in lost charges due to missing documentation, which translated to $370,000 in incremental revenue for the institution.

Further Opportunities

In addition to preprogramming and auto-documentation, infusion system–EMR interoperability generates several new opportunities:

- For clinicians in critical care units, computer monitor dashboards can provide an immediate snapshot of the patient’s condition, correlating time-stamped infusion data with the patient’s physiological data for use in determining next steps in treatment.
- For pharmacists, the patient-infusion device association necessary for interoperability makes it possible to monitor the actual status of each infusion, enabling pharmacy to enhance workflow planning for subsequent bags, identify infusions where rates have changed, and receive immediate notification of discontinued infusions.
- For finance, accurate start-and-stop time data (resulting from automatic documentation) can increase “hard dollar” reimbursement for outpatient, emergency department, and observation patient infusions.

Possible use cases are shown in Figure 4.

Going Forward

Closed-loop infusion device–EMR interoperability allows for enhanced patient safety, near-real-time surveillance, and charge-capture opportunities—benefits that are simply not available with standalone infusion pumps. To optimize use of these advanced infusion safety systems, hospitals and vendors need to think differently about support and sustainability. IT departments need to be better equipped to evaluate the unique performance challenges that infusion devices bring to the network.
support and sustainability. IT departments need to be better equipped to evaluate the unique performance challenges that infusion devices bring to the network.

The following examples describe how infusion device manufacturers and hospitals need to think differently when evaluating and maintaining a robust, integrated, interoperable system:

- Infusion devices are different from laptops, tablets, and many other devices on the network (Figure 5), and new processes and procedures may be needed to evaluate them effectively.
- Network performance criteria that were acceptable in the past may not be suitable when integrating infusion systems with the EMR.
- Infusion system vendors need to collaborate with hospital IT and HTM departments and offer 24-hour-per-day support for problem resolution and security updates.
- A new level of collaboration is needed among various hospital departments, as well as among those departments and the infusion device and EMR vendor teams.

**Implications for HTM and IT**

Just as technologies are no longer contained in “silos,” hospital staff can no longer limit their awareness and understanding to currently existing departments. Before interoperability, if a nurse said, “This pump doesn’t work,” the device went to HTM to be fixed. If pharmacy complained, “The new drug library won’t upload,” IT was called. However, after computerized physician order entry, BCMA, smart pumps, EMRs, and the hospital network are involved, the problem becomes much more complex. “I can’t program this pump” could mean that the device is broken, the signal at the wireless network access point is too weak, a portable X-ray machine is blocking the signal from the BCMA scanner to the infusion pump, the network is temporarily overloaded by other devices, the server or interface engine is down, or several other possibilities. Correctly identifying the problem becomes far more challenging. A much higher level of interdisciplinary understanding and interdepartmental collaboration is required to 1) solve the problem and 2) identify and remedy any underlying cause(s), so that the problem does not recur.

**Conclusion**

As previously described and further documented here, the journey to interoperability has shown itself to be worth the effort. Solving “the last 10 feet” for safe and efficient IV infusion medication administration is critical to improving patient outcomes and reducing unnecessary steps and waste. However, as summarized in the sidebar (next page), optimizing the benefits requires a change in mindset. Hospital staff
Figure 5. Traditional commercial off-the-shelf (COTS) technology–based clients versus pumps using device connection management protocol (DCMP): differences in communication and methods of securing data links. Top: Devices such as laptops and workstations incorporate widely used operating systems, human authentication, and varying degrees of encryption to communicate with diverse, often unsecure, resources. They also allow for the use of accessories, such as USB drives, that increase the system’s vulnerability to software viruses. Bottom: Intravenous infusion systems using DCMP leverage single point-to-point, bidirectional conversations and certified encryption with fewer user-centric variables, as compared with laptops and tablets. Only the infusion device can initiate a conversation with the server, using a secure conversation. Abbreviations used: AES, advanced encryption standard; IP, Internet Protocol; TCP, Transmission Control Protocol.

Current Summary of Lessons Learned and Best Practices Regarding Implementation of Infusion System–Electronic Medical Record (EMR) Interoperability

Medical device integration is a collaborative process.
1. Device security and data integration continue to evolve.
2. Device manufacturers and hospital IT and HTM staff need to work together to take advantage of a secure, connected, medical device system.

Best practice suggests that all concerned need to
1. Understand that the total project scope is more than technology alone.
2. Develop evaluation and security procedures to handle regulated connected devices that may not incorporate commercial off-the-shelf communication components.
3. Promote organizational changes and cross-training harmonizing HTM and IT support functions.
4. Require device manufacturers to scale and support for enterprise EMR connectivity.
need to view these unique devices as integral components of the EMR infrastructure. Meanwhile, the role of the infusion system company has changed from equipment supplier to long-range partner in monitoring and optimizing highly sophisticated, interoperable systems. Although Wi-Fi networks have improved dramatically in the last 15 years, the loads also have increased and the effort needed to ensure that wirelessly connected medical devices are safe and effective continues to be important.

References


