

'Where IT Meets IV'

Integrating Intravenous Infusion Devices With Hospital Information Systems

Dan C. Pettus and Tim Vanderveen

About the Authors



Dan C. Pettus is the vice president of connectivity solutions and IT support for CareFusion. E-mail: dan.pettus@carefusion.com



Tim Vanderveen is vice president of The Center for Safety and Clinical Excellence for CareFusion. E-mail: tim.vanderveen@carefusion.com

Since 2001, “smart” intravenous (IV) infusion pumps with dose-error-reduction software (DERS) have provided hospitals with critical safeguards against potentially fatal pump programming errors and a treasure trove of previously unavailable information on patient safety, IV practices, and quality of care. Nevertheless, IV infusion errors that result in harmful and even fatal adverse drug events (ADEs) are a continuing concern.

In response to numerous safety and performance issues with IV infusion pumps, the Association for the Advancement of Medical Instrumentation (AAMI) joined with the Food and Drug Administration (FDA) to host a summit on infusion devices in October 2010. As described in the subsequent conference report, *Infusing Patients Safely*,¹ a multidisciplinary steering committee was formed to lead a number of working groups in establishing priorities, developing guidelines, and identifying and sharing best practices to improve the safety of IV infusions.

Although the agendas of the various working groups are still being developed, the steering committee has adopted a set of future vision statements to help guide it and the working groups in their efforts to make IV infusions safer. The vision boldly describes an attainable state and sets an aggressive national agenda to capitalize on the present opportunities, stating as its mission that “no patient will be harmed from a drug infusion.”

The vision starts with establishing wireless

connectivity between a hospital’s hundreds of infusion pumps and the hospital’s wireless network. Without this connectivity, other significant advances for improving infusion safety will be impossible to achieve. With this connectivity, an exciting new state of greatly improved safety, quality and productivity can be attained.

This article is based on vendor experience in working with hospital partners to implement wireless connectivity for more than 300,000 infusion devices on wireless networks across hospitals of all sizes and levels of complexity. The benefits, challenges and opportunities of integrating infusion devices into hospitals’ health information technology (HIT) systems will be addressed, along with ways to meet the challenges. The potential impact of the continuing convergence of clinical engineering and information technology (IT) will also be covered.

IV Infusion Pumps

Infusion pumps have been in use for more than four decades and typically are the most widely used medical devices in hospitals and other clinical settings. While most medical devices are monitoring devices that provide specific data about each patient, infusion pumps are programmed devices that provide therapy to specific patients. Most medical devices that require programming are therapy-specific devices such as hemodialysis, balloon pumps, and coronary bypass machines that are operated by highly skilled clinicians and technicians. Infusion pumps, which are used to administer

hundreds of different types of medications, including many of the highest-risk drugs, are used by virtually every nurse in a facility, with varying levels of skill and experience.

For the first three decades of their use, infusion pumps placed no restrictions on clinician programming of rates, volumes, or doses. Within the performance range of a pump, any programmed parameters were “OK,” even if they constituted a massive overdose or underdose for the particular patient being infused. The pumps were essentially individual islands, with no way of knowing who they were being used on, who was using them, or their intended use. Important safeguards were needed.

Smart Pumps

In the early 2000s, computerized IV infusion pumps with DERS—so-called smart pumps—began to appear. These new devices had extensive software drug libraries that reduced programming steps and provided standardized concentrations, dosing units, and a variety of alerts to warn clinicians of possible programming errors. Initially, updating the drug libraries presented major challenges, since this required that a technician physically touch each device to manually upload a new drug library using a laptop connected to a serial port on the pump.

Some smart pumps also logged the data on each safety-software alert and the subsequent action by the caregiver, including reprogramming, overriding soft limits, or cancelling the infusion altogether. Typically the logged data were downloaded or a revised drug library uploaded by clinical engineering during the annual or semiannual preventive maintenance. Analysis of the six- to 12-months’ worth of downloaded data was not completed until long after the preventive maintenance was done. If the data analysis showed that changes needed to be made to the safety software (adjusting limits, adding new drugs, etc.), often this was not done until the next round of preventive maintenance, six to 12 months later. Thus, the implementation of necessary changes was greatly delayed, which had direct, negative impact on compliance, attention to alerts, protection for new drugs, and changes in therapeutic use.

Wireless Connectivity

The introduction of wireless connectivity for IV pumps in 2004 represented a major advance in

IV infusion medication safety. Alert data could now be collected and analyzed at any time, and an updated library could be transferred directly to every pump in the hospital whenever necessary over the wireless system. Wireless integration also opened up new possibilities for improving the safety and quality of IV infusion therapy. In addition to reducing the likelihood of medication errors, wirelessly connected smart pumps could help improve charting by making documentation an automatic by-product of a nurse’s workflow. Auto-programming is also made possible by wireless connectivity.

In the small number of facilities that implemented auto-programming as of this writing, the physician’s order goes directly from a patient’s electronic medical record (EMR) to the infusion pump to populate the correct parameters for infusion, thereby eliminating the opportunities for error associated with manually programming the pump. However, the infusion systems still need to maintain their internal safety software, since many IV orders require the nurse to adjust (titrate) the dosing parameters during the course of a single order. Protection from overdosing or underdosing during titration will continue to be provided by the pump’s internal safety software.

Auto-programming and automatic documentation streamline workflow and increase the efficiency of medication use, enabling clinicians to have more time to do what they were trained to do: direct patient care. Wireless connectivity supports information capture and sharing and, as described above, facilitates technical support.

Wireless connectivity also makes possible remote surveillance of infusions in progress by the patient’s caregiver, physician and others, whether they are at the bedside, a nurse’s station, in the pharmacy, or in another location. Serious injuries and even deaths can be averted when others can know that a ten-fold overdose alert has been overridden, an IV is still infusing after being ordered to be discontinued, or critical alarms and alerts have been missed.

Server-based data-management applications can track and manage hundreds or even thousands of infusion devices enterprise-wide. The server uses the hospital network to reach wireless access points, which transmit updated data sets each time they are in contact with an infusion device. At the same time, the system downloads the alert logs stored in the smart

For More Information

To learn more about AAMI’s initiatives related to infusion device safety, visit: www.aami.org/hottopics/infusion%20pumps/index.html.

In addition to reducing the likelihood of medication errors, wirelessly connected smart pumps can help improve charting by making documentation an automatic by-product of a nurse’s workflow.

Requirement	What's Needed	Comments
Infusion pump drug library update	Batch data push	Real-time not required. Batch updates can be optimized in the infusion pump software
Infusion pump status (Flowsheet and status board population)	Semi Real-time	A few minutes between updates are acceptable. Infusion pump software can help with small efficient data packets
Infusion pump alarms push	Almost real-time. High Quality of Service (QoS) mission critical	Less than one minute end-to-end. Validate and display connectivity status, so nurses are aware of a pump that is not communicating for whatever reason
Infusion pump auto programming	Near Real-time. High QoS mission critical	Within seconds end-to-end. Validate and display connectivity status, so nurses are aware of a pump that is not communicating for whatever reason

Table 1. Wireless Requirements for Infusion Pump Integration

infusion systems, providing a continuous stream of clinical data for analysis to identify opportunities for quality and best-practice improvements.

Challenges

Integrating so many wireless devices into a hospital's IT infrastructure presents challenges as well as opportunities. The challenges of achieving infusion system-wide integration include cost, technology, implementation and culture. Of these, cultural barriers are the most difficult to overcome.

Cost: Technology costs, a frequently cited barrier, can be justified by the return on investment (ROI) generated by reducing the likelihood of serious, costly ADEs through safer delivery of high-harm medications and by optimizing pharmacy and nursing workflow through real-time surveillance of IV infusion processes. Reducing serious medication errors decreases length of stay; providing pharmacy with a window to each bedside helps the staff to better plan workload and reduce waste; and providing nurses with remote alarm and alert management helps them provide better care and avoid unwarranted outcomes. These are all examples of solid returns that can be obtained from these technology investments. Cost reductions can also result from minimizing the number of disparate protocols and infrastructure requirements for different infusion modalities.

Having to support multiple infusion connectivity strategies from multiple vendors can be a technical and resource-allocation challenge. The ideal infusion device would have a single wireless radio, a common software protocol and a common platform that could combine any of

the different infusion types (large-volume, syringe, and patient-controlled analgesia [PCA]) at the point of care, so that the networked pumps would use a single server, and the infusion safety system would be easy for the IT staff to administer. Reducing the number of different devices from different vendors for different types of infusions simplifies system implementation and maintenance, reduces opportunities for errors, lowers costs and increases productivity.

Technology: Most hospitals' current wireless systems are based on standards that were never designed to support such connectivity. Consider the mobile phone: Who could have predicted how far these devices would go in using data assets beyond making a simple phone call?

The demand for mobile appliances within the walls of the hospital is now enormous. A wireless-enabled infusion system must be a "good citizen," share the wireless highway with others and not take up all the available bandwidth. Table 1 summarizes the potential different wireless requirements based on infusion systems' needs.

The level of service required varies widely, depending on the connectivity function. That being said, any hospital wanting to have a wireless system that incorporates infusion safety systems should plan for full auto-programming, since this important safety capability will undoubtedly become widely available over the next several years. Auto-programming requires both the necessary technology (near-real-time wireless connectivity) and a fundamental change in clinical workflow at the point of care to associate the device to a patient and a caregiver to the device. It also requires image recognition (currently barcode scanning) to initiate the programming process.

Understanding the infusion systems' need for bandwidth, network latency, and wireless security are some of the obstacles that can and must be overcome with proper planning and design.

- **Bandwidth.** Infusion systems' need for bandwidth can be minimized with proper design of the infusion pump software. One example is to minimize wireless payloads by using event-driven protocols that send and receive data only when required. Another is to reduce the data packet size by encoding data in bits, not bytes. This not only reduces the packet size but also increases security by transmitting non-"clear text" over the network.

The challenges of achieving infusion system-wide integration include cost, technology, implementation and culture. Of these, cultural barriers are the most difficult to overcome.

- **Latency.** An integrated infusion system will require an allocation of wireless bandwidth and communications-turnaround times (latency time) that are appropriate for its intended use. For example, deploying infusion pumps on a wireless network in order to update the drug library may require only a small amount of bandwidth, and latency times would not be that important. However, deploying or upgrading infusion systems for near real-time activities such as auto-programming will require short wireless-latency times and periodic increases in bandwidth utilization.

Implementing infusion-pump connectivity in a complex wireless ecosystem can be a daunting task. However, if managed well, it can be accomplished with minimal disruption to workflow and resources. A good start may be to perform a risk assessment and document the findings using the IEC 80001 process. Another method to achieve good results with infusion-pump wireless connectivity is to incorporate the same requirements that have been established for Voice over Internet Protocol (VoIP).

- **Security.** Maintaining security and safeguarding privacy are major concerns in integrating IV infusion devices with a hospital's wireless network. For the most part, medical devices do not support off-the-shelf operating systems, so processes such as updating virus databases or patch management are not applicable. One of the best ways to ensure reliable and secure device integration is to require the device vendor to provide evidence that the device's reliability and security have been certified by an independent third party. For medical devices such as wireless infusion systems, the government has developed a testing method that is certified by the National Institute of Standards and Technology (NIST). This certification test is called Federal Information Processing Standard (FIPS) 140-2 and should be a minimum requirement for any medical device integrated into a complex hospital wireless environment. Although FIPS 140-2 is strictly focused on the cryptographic modules, it presents a good starting point, since no other official certification process exists in today's market.

A list of certified vendors can be found on the NIST website.² A list of suggested qualifying questions and proof points to help in vendor selection are shown in Table 2.

Qualifying Questions
Have the pump wireless cryptographic techniques been certified by NIST to comply with FIPS 140-2 security requirements?
Has a qualified third party validated commercial security technology and procedures?
Do the server and network administration have clearance from the FDA as medical devices aligned with new MDDS rules?
Will the pump limit RF output on infusion device to lowest power necessary?
Does the pump vendor have an established software patch management process?
Did the infusion system vendor implement server hardening techniques? How?
How does the infusion system minimize transmission load on network?
Will the pumps function clinically regardless of wireless connection state?
How does the infusion vendor lock down server administration accounts?
Will the infusion system vendor provide 24/7 remote server health and monitoring?
Describe how the infusion system will leverage existing hospital active directory services.
How many infusion types (modalities and channels) can be combine on a single, secured, wireless channel?
Indicate the number of infusion pump channels per single server instance.
Ask the vendor how many wireless infusion channels are commercially installed and operational.

Table 2. List of Qualifying Questions

Implementation: Integrating infusion pumps with other hospital IT systems opens up both new opportunities and potential problems. To maximize the opportunities and minimize the problems, a vendor should have a mature project management team that can work well with the staffs of the various departments involved in the implementation process, including nursing, pharmacy, clinical/biomedical and IT. Understanding and providing solutions to the challenges of workflow changes and using established approaches to project management and oversight have been shown to be a proven formula for success.

Culture: In the past, acquiring a new infusion system typically was a clinical and materials management departmental decision that required little involvement of any other disciplines. The integration of infusion devices with core HIT systems changes that. Skills and subject expertise from both clinical engineering and information system professionals are now required.

Where "IT meets IV" is a convergence of more than just two different types of technology. The success and ongoing value of wirelessly connecting smart medical devices to a hospital's IT network depends entirely on the increasing convergence of clinical engineering (biomedical engineering) and information systems. IT needs to better understand the role of medical devices

One of the best ways to ensure reliable and secure device integration is to require the device vendor to provide evidence that the device's reliability and security have been certified by an independent third party.

within the hospital IT infrastructure and embrace the knowledge of clinical engineers. Clinical engineering needs to respect the role of hospital IT and embrace the need to demonstrate how the medical device will operate in the network environment and then to provide the subject expertise to resolve any connectivity, security or network administration issues such as patch management.

The device vendor has the responsibility to design its devices to fit neatly into current IT infrastructures with high reliability and security. The clinicians that use these new technologies must be actively engaged from the beginning in developing the network-device solution. New workflow schemas cannot be “forced” on the clinical staff or they will not be adopted. From day one nurses, pharmacists, and clinical administrators will need to understand the implications of changing from manual workflow and isolated devices to the automated processes of wireless connectivity.

Suggested Best Practices

- Develop a long-term strategy for medical device wireless integration.
 - Ask: Will what I’m doing today enhance or block future value of a connected strategy?
- Promote the convergence of clinical and IT domains.
 - This requires unique skills and may require new job titles.
- Validate security and performance.
 - Ask: Has there been qualified validation of wireless security and performance?
- Be flexible; be ready.
 - Value of connectivity for improved safety and efficiency is extremely high.

Meeting the Challenges

The good news is that many hospitals will be able to adopt full infusion-pump integration and provide high-quality functionality on the wireless infrastructure for years to come.

However, this will not happen by accident. In particular, the following best practices are needed to help meet these challenges:

- Wireless infusion devices must be designed for the 802.11 networks with a full understanding of the technical requirements for roaming, bandwidth, security, and resynchronization of data.
- An infrastructure vendor must cooperate by providing highly reliable wireless components that are not proprietary and adhere to the 802.11 specifications.
- Hospital IT departments need to develop a long-term strategy for medical device integration and have a good understanding that most medical devices do not operate like desktop, off-the-shelf systems. Successful integration of medical devices may even require additional personnel who are subject experts in both clinical engineering and enterprise IT.

Conclusion

The introduction of wireless connectivity between smart pumps and a medical-grade server in 2004 was an important advance that

allows for easy transfer of DERS library updates to every device in a hospital and frequent collection of the CQI log data. Wireless connectivity also provides the technology needed to develop advanced interoperability between biomedical devices and IT. As with any wireless device on a hospital IT network, security against hacker and network breaches needs to be addressed and evaluated. A multilayered encryption architecture helps protect the privacy and security of the transmitted data and is considered a basic requirement for infusion pump deployment in a wireless infrastructure.

The potential value of a wirelessly connected infusion system for improved safety and efficiency is tremendous—the ability to provide surveillance of running infusions from anywhere and when needed, to update drug libraries at will, to automatically populate the electronic medical record, to electronically automate the medical order for infusion administration—and the list continues to grow.

Experience has shown that the process of integrating advanced smart devices with a hospital’s information systems can catalyze the development of a culture of collaborative systems thinking with greater standardization and consciously designed processes that free nurses to spend more time with patients.

To achieve the ultimate goal of a fully integrated infusion safety system, clinical engineering and IT professionals will need to work together, understand each other’s needs, and recognize that their disciplines will continue to converge. This will undoubtedly present both cultural and technological changes. However, if such changes are embraced, the results can be remarkable. ■

References

1. **Association for the Advancement of Medical Instrumentation.** Infusing Patients Safely: Priority Issues From the AAMI/FDA Infusion Device Summit. 2010. Available at: www.aami.org/infusionsummit/AAMI_FDA_Summit_Report.pdf. Accessed June 10, 2011.
2. **National Institute of Standards and Technology.** Validated FIPS 140-1 and FIPS 140-2 cryptographic modules. Available at: <http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2011.htm#1543> Accessed June 10, 2011.