Medical Device Connectivity for Smarter Healthcare

Real World Integration – Applications, Integration Issues and Benefits

Lantronix, Inc.
7535 Irvine Center Drive, STE 100
Irvine, CA 92618
Tel: +1 (800) 422-7055
Fax: +1 (949) 450-7232
www.lantronix.com

Contents

Introduction

The need to optimize healthcare operations, manage operational costs, and improve patient experience has sparked increased interest in the benefits of medical device connectivity. It also has created a demand for information about specific implementation requirements for some of the key applications that are poised to take advantage of data communications networking across medical equipment. In this paper, we will discuss five key applications for medical device connectivity, focusing on requirements, implementation, and associated benefits. These five application areas are: OR/anesthesiology, ICU bed, patient room, lab environment/printers and mobile cart. This paper will also discuss the challenges specific to wireless integration.

What is Medical Device Connectivity?

Virtually every medical device has what is called a serial or communications port for sending data from the device to another piece of equipment or network. Basically, medical device connectivity involves getting that data onto some type of network so that it can be integrated with an EMR system. This can be done in two ways either through a built-in network port on the device or an adapter. If the device is fairly new it may have a network port built into the unit. However, in some cases, you will need to use an adapter on the serial output port to network-enable the device. Medical devices typically have a long product life cycle and making hardware changes to existing equipment from the factory will require months to get approval from the U.S. Federal Drug Administration (FDA).

To better understand the use and implementation of medical device connectivity, we need to first look at the specific applications. These are some of the primary applications where the ability to network medical devices provide real value but the requirements and integration of each one can differ slightly.

We will review the applications based on acuity from high to low. In critical environments, the need to maintain high acuity with real-time monitoring of large amounts of data simultaneously with the highest level of detail. As we move down the list, the urgency and complexity of the integration lowers at each level.

OR/Anesthesiology

This is the highest acuity application for medical device connectivity. In an operating room (OR)/anesthesiology environment there are typically a host of monitoring and life sustaining devices in use at one time. It can also be a fairly harsh environment for equipment, which includes exposure to saline solutions and other fluids. This application area typically will require a well-sealed network connectivity unit that provides 8 to 16 ports to accommodate all of the medical equipment in use. It's typically a wired network application, although there is some discussion about moving to wireless technologies as new medical devices are launched.

ICU Bed

This is often a high acuity environment with similar requirements to the OR/anesthesiology application. Since much of the equipment is stationary it usually requires a wired unit with anywhere from 8 to 16 ports.

Patient Room

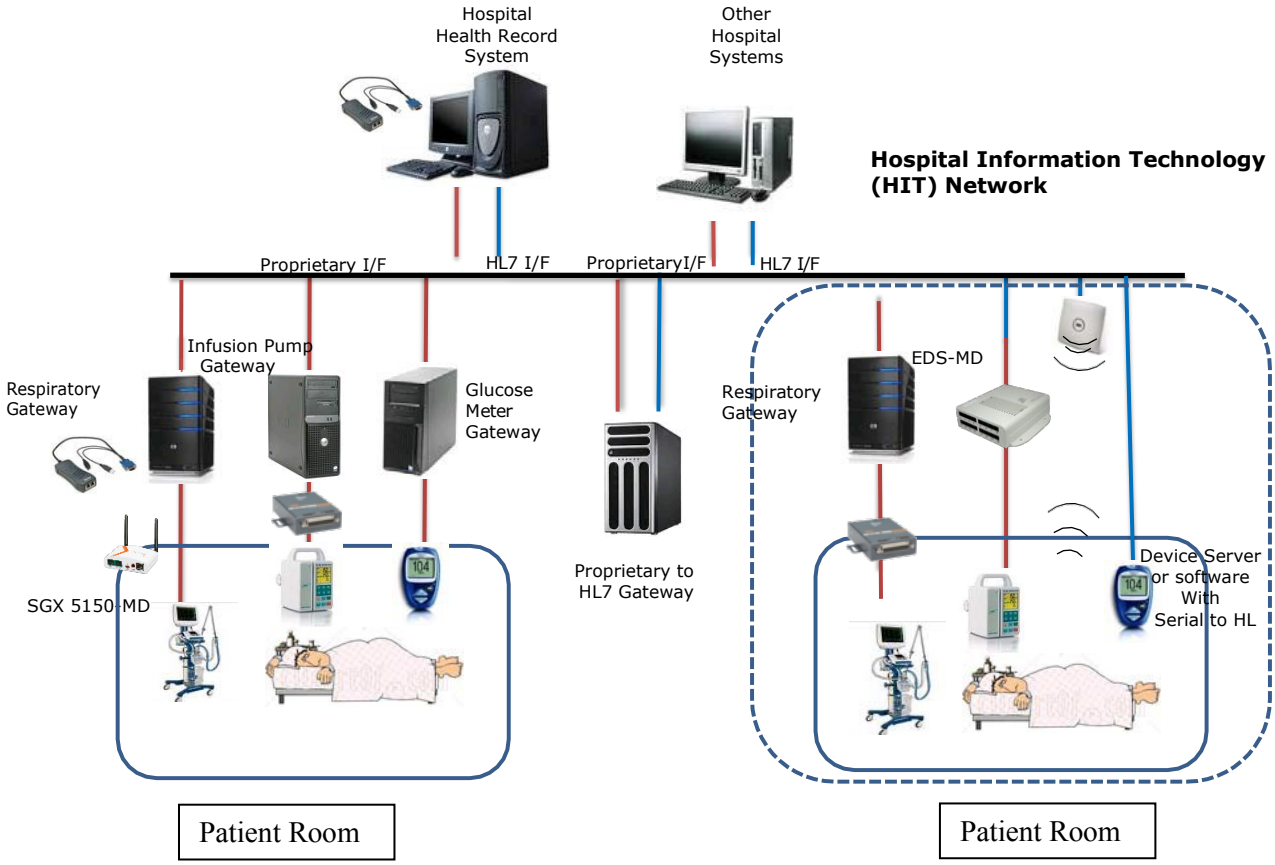
This is a lower acuity environment compared to the ICU with fewer monitoring devices since the patient is on the road to recovery. In this application the connectivity can be wired or wireless with typical port density requirements of 4 to 8 ports.

Lab Environment/Printers

The requirements for the lab environment are generally not as critical as those for patient areas in a hospital. Typically, these devices are found throughout health-care organizations. In many cases, lab device connectivity is performed via single- or dual-port devices with either a wired or wireless connection. These devices usually do not require any special drivers and the connection is often quite simple once the basic connection settings are configured.

Mobile Cart

Mobile carts are used throughout the hospital environment -- patient rooms, lab areas and emergency rooms, etc. -- to perform medical tests as needed. Typical devices include glucose monitors and portable heart monitors. These devices require a wireless connection to the network since they are always on the move. In some cases, these devices are battery powered so power consumption can be an important consideration. An additional benefit of network enabling these devices is asset tracking to help locate them in the hospital or clinic.



Key Benefits

While each application reaps its own set of benefits thanks to network enabling, there also are shared benefits across all applications ranging from greater efficiency and accuracy to ensuring patient privacy. Here's a quick rundown of some of those shared benefits:

Greater efficiency and accuracy

Instead of nurses manually logging patient information in paper chart records at the bedside and later transcribing the data into a computer, the data is automatically uploaded to the patient's electronic record, eliminating the possibility of human error.

Cost savings

It increases staff productivity by eliminating hours of time spent on administrative duties. Since all patient data can be stored in one electronic record, billing becomes much more automated and streamlined further reducing costs and errors.

Better quality of care

Freeing the staff from the administrative duty of manually inputting data gives them additional time to focus on patient care. Automation also allows for better response to alarms and finer detail in tracking patient data. It also provides doctors or other care givers with instant access to a patient's health status from just about anywhere with a network connection, eliminating the need to review a physical patient chart**.**

Patient privacy

Since the records can be sent over an encrypted connection there is no paper to be lost or fall into the wrong hands, ensuring only those that are supposed to have access to the data are allowed to see it.

Integration Issues

As is the case with the benefits of device integration, the issues faced when trying to integrate these products are similar across the different applications. In general, the highest acuity applications have more complex integration issues than the lower acuity areas, but they share many common challenges.

Physical Connection

The first issue is basically one of plumbing. How do you physically connect the

devices? As discussed earlier, virtually all electronic medical equipment feature a port for output of the data but that is where the similarity ends. Each physical port can be one of at least seven different types of common connectors. The most common include 9-pin male, 9-pin female, 25-pin male, 25-pin female, 37-pin male, RJ45, and RJ11. These are in addition to proprietary connections from some manufacturers.

In addition to the physical connection, there are several communications protocols as well as basic setting requirements such as baud rate, data transmission rate, parity settings for error checking, stop bits, character size (number of bits -- 7 or 8 -- per character), and flow control that need to be considered. While all of these settings and characteristics can vary by manufacturer, many of them use the same pin-out standards

We have included a table at the end of the article that outlines many of the common connections.

As daunting as all of this seems, network enabling your medical equipment is not as difficult as it may seem as long as you take a step-by-step approach. The first step is to select the connector type. From here, you can determine the pin-out from the chart below. Most manufacturers will list the required communication settings in the manual. Once completed, you should be able to start basic communications with the device.

However, it is important to note that there will be some key implementation and requirement differences among the six applications listed above.

As an example, OR/anesthesiology/ICU and patient bed applications have the highest level of integration issues due to the variety of different devices and manufacturers involved. In addition to the serial communications protocol, there is an application layer protocol that addresses the data transmission from the medical devices, which will differ across each manufacturer and each type of device.

For example, the data transmitted from an EKG machine will be very different than the data from a ventilator or an infusion pump. In order to interpret that data into a meaningful output, some type of driver or conversion will be required.

There are several initiatives underway to make this an easier process. One is the IEEE 11073 initiative that sets the standards for how medical devices communicate. This standard provides subsets for each type of medical device, so the standards for all equipment will differ. It will significantly help with the integration of new products going forward but still requires the need for some type of driver.

The other initiative is HL7, a gateway approach to transmitting data, which converts the data stream from the device into a HTML output that can be easily understood by many EHR software packages.

The IEC 60601 Standard

Medical devices and equipment are highly regulated, and they are held to a higher level of safety than most other types of equipment on the market. The obvious reason for this is that medical equipment is used on human patients.

One of the most important questions that often arises with the integration of a medical device is the need for IEC 60601 compliance. IEC 60601 is an internationally harmonized safety standard that allows medical products to be designed and evaluated for compliance under a single standard. This standard is also eligible for use in many different countries. In addition to being the base of so many harmonized standards, IEC 60601-1 is a FDA recognized consensus standard that is used to support a manufacturer's declaration of conformity.

The purpose of the IEC 60601 standard is to ensure patient safety. To comply with the standard, medical equipment must be safe to use under both normal and single-fault conditions. There are four distinct parts of the IEC 60601 standard. They are as follows:

- IEC 60601-1 covers all the general requirements for electrical medical products.

- IEC 60601 -1-x collateral standards cover horizontal issues such as EMC testing for a variety of medical devices.

- IEC 60601-2-x covers requirements for a specific type of medical device. For example, IEC 60601-2-2 is the standard for high-frequency surgical devices.

- IEC 60601-3-x covers performance requirements for a specific type of device.

The collateral standards also include requirements for specific technologies and/or hazards:

- IEC 60601-1-1 Medical systems

- IEC 60601-1-2 EMC compatibility issues of electrical medical devices

- IEC 60601-1-3 Radiation protection

- IEC 60601-1-4 Software

Determining if a medical device falls under the IEC 60601 standard can be a complex task. Electro-medical products are defined in IEC 60601-1 Sub clause 2.2.15 as: *". . . equipment, provided with not more than one connection to a particular supply mains and intended to diagnose, treat, or monitor the patient under medical supervision and which makes physical or electrical contact with the patient and/or transfers energy to or from the patient and/or detects such energy transfer to or from the patient."*

Examples include MRI and gamma imaging systems, infusion pumps, vital sign monitors, battery-operated thermometers, and endoscopic cameras.

To achieve international approval can sometimes be tricky. Most major countries have adopted IEC 60601-1 as a national standard. However, each country has its own safety and regulatory agencies and, in some cases, a national standard for local requirements.

Conscientious vendors need to keep up-to-date with the IEC60601 certification. Ensuring that the latest edition of certification is used, this narrows down the choice of potential solutions that are in compliance with the latest standards. Selection of vendors that keep their products up-to-date with the newest edition provides a far better level of assurance with deployments in environments that mandate this due to regulatory requirements that require moving to the newest edition of the certification.

Application Challenges

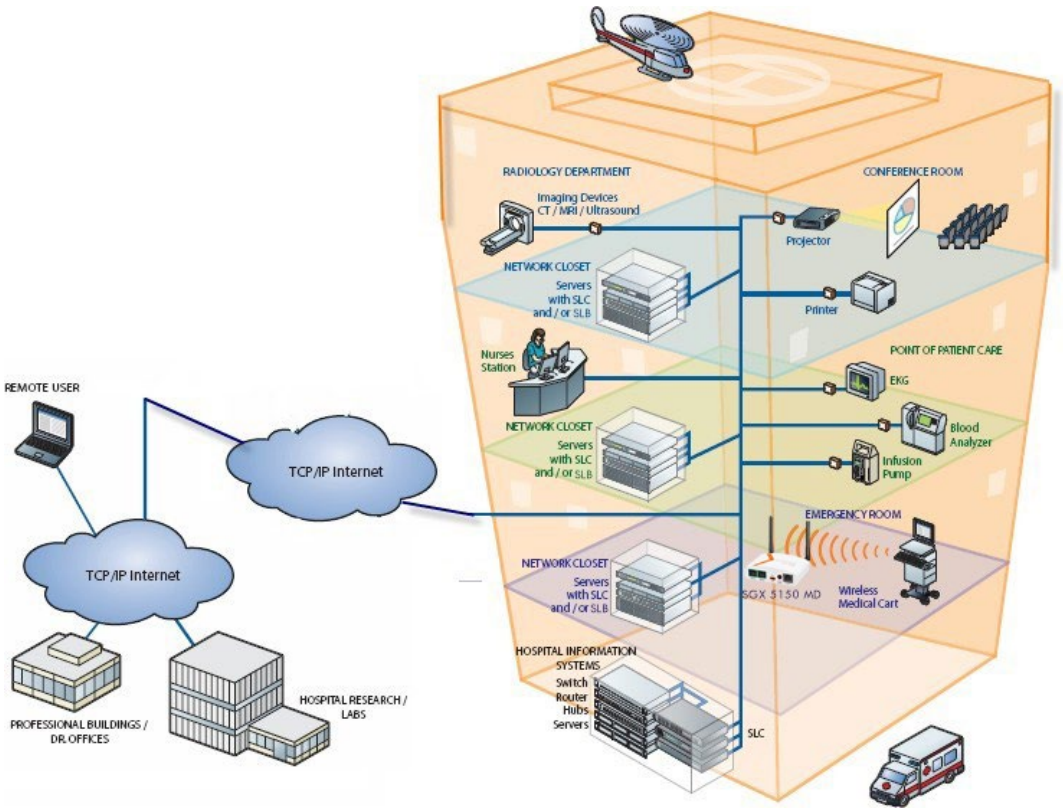
The IEC 60601 requirement for medical device connectivity is one integration issue that comes into play primarily in the OR/anesthesiology and ICU/patient bed applications. Many hospitals view the standard as an unnecessary cost while some others consider it a requirement.

However, in the lab environment, integration issues are more flexible. IEC 60601 is not an issue in the lab since there is no patient interaction. These lab devices also are less complex than those found in the ICU or OR and the data stream is more defined.

Still, the same physical connectivity issues apply as they do in other applications. In most cases, lab equipment is designed to be connected to a computer, but connecting each device can be an expensive and complicated task. One low-cost solution to access all of the lab equipment from one location is to use a small external device server. A main server can then be equipped with a piece of software known as a serial port redirector. This software basically makes the computer think it is directly connected to the serial port on the device via a serial connection when it is, in fact, connected over the network. This allows the computer to utilize the software intended for direct connection and to communicate with multiple devices.

The mobile cart or device market brings up a host of other integration issues, specifically related to wireless technologies. Since wireless has its own set of integration issues we have devoted a specific section to wireless later in the white paper.

While a wired connection is very easy to implement if the cabling and infrastructure is in place, it does have some limitations with regards to flexibility if the necessary cables are not already in place or if the unit needs to be mobile. Wireless integration is significantly more complicated, so we will next delve into the intricacies of different wireless implementations.



Wireless Integration Challenges

Medical device manufacturers are starting to realize the benefits of adding wireless technology to their products that will allow health-care organizations to remotely monitor and access their devices. For many companies, the reality includes a host of challenges associated with its implementation. This is largely due to the list of requirements necessary for creating a true wireless solution. Chipsets and drivers that are difficult to integrate are required, as is a strong understanding of RF and TCP/IP networking among other technologies. In addition, the daunting task of FCC certification is a rigorous and time-consuming process. Security is another major concern. It has been argued that wireless is not as secure as other networking alternatives.

However, it can be just as secure as wired technology with the use of the latest encryption and authentication algorithms. It is important to note that when implementing wireless technology, each application features its own set of challenges and requirements. These are just a few of the obstacle's health-care organizations may face when implementing a wireless solution.

A significant amount of engineering expertise is needed to effectively implement an IEEE 802.11 a/b/g/n/ac interface into a medical device that is dual-band and supports both 2.4GHz and 5GHz. In crowded hospital environments the 5GHz is strongly recommended to improve performance. The following are some of the high-level details on how to implement an

802.11a/b/g/n/ac Wireless Local Area Network (WLAN) solution including design trade-offs, hardware/software integration, FCC approvals and enterprise wireless security.

Medical WLAN system design tradeoffs

Implementing a medical WLAN interface is a very challenging assignment partly because there are so many design details and trade-offs that must be considered such as:

- What is the required security of the WLAN link?
- What is the right radio spectrum to use?
- What is the required range of the WLAN connection?
- What data throughput is required?
- What is the available power versus power consumption?
- How do you get regulatory approval for the wireless device?

Every medical application is different. Depending on the requirements, these trade-offs can have a big impact on design choices. Before any design work can start, these questions should be reviewed and answered.

What is the required security of the WLAN link?

Wireless security is an important issue and a valid concern. There are two elements to security: encryption and authentication. Encryption involves scrambling the data prior to transmission to prevent someone from viewing it in clear text. Authentication is a process that determines whether a client radio is authorized to connect to the wireless network. IEEE 802.11 a/b/g/n/ac standards provide a range of security options. Several off-the-shelf wireless solutions provide these security algorithms as a built-in option.

For 802.11 a/b/g/n/ac networks, the first attempt at securing the wireless link was Wired Equivalent Privacy (WEP). WEP provided very light authentication and weak encryption to scramble the data, resulting in successful attempts at breaking the security. The 802.11 committee responded with the creation of the 802.11i standard, but for a variety of reasons, this effort took longer than expected.

In the meantime, the Wi-Fi Alliance created an industry standard called Wi-–Fi Protected Access (WPA). WPA, which solves many of the problems associated with WEP, was designed for use on most access points or client station radios that were currently running WEP. This made for a quick and easy migration.

Although WPA was designed for use with an 802.1x authentication server, which distributes different keys to each user, it is most commonly used in a less secure personal or "pre-shared key" (PSK) mode. Data is encrypted using the RC4 stream cipher, with a 128-bit key and a 48-bit initialization vector (IV). One major improvement in WPA over WEP is the Temporal Key Integrity Protocol (TKIP), which dynamically changes keys as the system is used. When combined with the much larger IV, it can defeat well-known key recovery attacks on WEP.

IEEE 802.11i/WPA2 security offers all the capabilities of WPA but further improve security by replacing the RC4 algorithm with the Advanced Encryption Standard (AES) for data encryption. AES provides enough security to meet the requirements of the Federal Information Processing Standard (FIPS) 197 specification, which is required by many government agencies.

802.11i can be used in two different modes: Personal and Enterprise. Personal (or PSK mode) is intended for home and small medical office networks that cannot afford the cost and complexity of an 802.1x enterprise authentication server. Enterprise mode is used typically for larger installations in hospitals and other large medical facilities. In enterprise mode, IEEE 802.1x is used for authentication, authorization, and accounting. It uses the Extensible Authentication Protocol (EAP) mechanism for authentication. There are several protocol variations of EAP, but the two most popular in use today are Protected EAP (PEAP) and Tunneled Transport Layer Security (TTLS). In many older hospital environments, Cisco LEAP (a lightweight EAP) is still in use; however, LEAP is not considered secure and is not part of the IEEE802.11i standard.

To implement enterprise security, the infrastructure needs a RADIUS Authentication Server. The most common radius server applications are Microsoft Windows 2003 Server with IAS, Funk Odyssey (needed for TTLS mode) or Open Source with FreeRADIUS.

One of the biggest integration issues with enterprise security is that the RADIUS server must have a server-side x.509 digital certificate. This certificate can be purchased from a third-party certificate authority such as Verisign, or it can be issued from an organization's internal certificate authority.

A third-party digital certificate typically costs about $500 per year and requires a Public Key Infrastructure (PKI) in place to verify the certificate. A very common way to get around these issues is to use a self-signed certificate on the RADIUS server. It is not as secure as the other options but still offer a high degree of security.

What is the right radio spectrum to use?

In the U.S., there is unlicensed spectrum -- called ISM bands -- at 900, 2400, and 5800 MHz. Choosing the desired RF frequency is generally the first task when

designing a WLAN interface. Today, the 2.4-GHz band comes closest to a true worldwide solution, thus it boasts the largest number of users. As a result, it is overcrowded and subject to much radio interference, driving most hospitals and medical facilities to migrate to the 802.11 a/n networks to use the 5-GHz spectrum. The 5-GHz spectrum provides many more channels with less interference, but the drawback is its shorter range. The best solutions are using multiple band radios (a/b/g/n/ac) to provide the most flexibility for application-specific requirements.

What is the required range of the WLAN connection?

Range is defined as the maximum distance between two transceivers that provides a minimum signal-to-noise ratio (SNR) to support a communications link. Range is frequently an important parameter to a wireless design. Unfortunately, it is one of the most difficult parameters to specify because the effective range of a wireless link is impacted by many variables. The following are the major factors that determine the range of a wireless link:

- Output power
- Gain of the transmit antenna
- Receiver sensitivity
- Gain of the receiver antenna
- Interference or noise
- Transmit frequency

Obviously, a longer range can be achieved with higher transmit power, but for battery applications, this will also increase power consumption. In some cases, if the radio has already received FCC approval, then the output power cannot be changed without additional FCC testing.

RF interference can impact the range and the quality of the link in several ways. In the presence of a noisy environment, WLAN radios will attempt to slow the transmission speed to achieve better receiver sensitivity. Also, since every message is acknowledged, there will be more garbled messages transmitted. Message error checking will catch these errors and force a re-transmission; however, this will slow down data throughput significantly.

Range will also suffer because RF interference will raise the noise floor and make it more difficult for the receiver to extract the intended good signal. In the 2.4-GHz spectrum, there is a fair amount of crowding from other 802.11 users as well as interference from other devices such as microwave ovens and cordless

telephones. Given this, it is important to estimate the worst-case RF environment in which the radio must work as well as the tolerable level of interference.

What data throughput is required?

Designing a radio to support the required throughput is an important part of the system design. The maximum data throughput is dependent on the amount of RF spectrum available, the RF modulation technique used and the transport protocol. For the majority of standard wireless protocols like 802.11, these parameters are part of the standard. Data throughput speeds range from 1 megabit per second (Mbit/s) to 1 gigabit per second (Gbit/s).

At the system level, the maximum data throughput can also be impacted by the host processor speed. Depending on the wireless solution, the processing requirements on the host processor vary and can have a significant effect on the overall performance of the wireless link. Some chipsets require very little intervention on the part of the system's host central processing unit (CPU), while others require host CPU processing cycles in the execution of WLAN operations. This can slow data throughput significantly and limit the bandwidth of the host CPU for other product tasks.

Data throughput requirements also impact the wireless technology selected. Is the data response time critical? Are there large quantities of data packets that need to be transmitted or received?

For example, Zigbee is limited to small data packets but the processing and power consumption requirements are lower. In comparison, 802.11 provides large data frames (up to 1472 bytes of data) but requires more processing and power consumption.

What is the available power versus power consumption?

Wireless communications can eliminate restrictive data cables and provide mobility for medical devices. But in many medical applications, to achieve that mobility, the power cable must be eliminated as well. Therefore, if the design requires mobility, then battery power is the best option. To achieve a reasonable operating battery uptime, power consumption of the overall RF circuit will be critical. Lower power consumption improves battery life but is often a trade-off with performance. Most WLAN devices offer power management and sleep modes to provide good battery life.

How do you get regulatory approval for the wireless device?

IEEE 802.11a/b/g/n/ac devices use the 2.4-GHz and the 5-GHz ISM license-free spectrums, which mean they are allocated for public use provided that certain

rules are followed. In the U.S., these rules are enforced by the FCC. The FCC requires any device that radiates RF energy in the license-free bands to be tested for compliance to CFR 47 part 15. Once the product reaches a finished prototype stage, a test lab can conduct the FCC part 15 compliance testing. In Europe the EU-RED standards are enforced for Wi-Fi and Bluetooth devices.

If the wireless device (such as a mobile heart monitor) will be worn by a patient, then Specific Absorption Rate (SAR) will become a very important issue. SAR is a measure of the heating value of radiated RF energy on the human body. SAR testing evaluates the relative safety of low-power RF transmitters when used in a close proximity to the human body. SAR requirements and testing are complicated issues and are beyond the scope of this paper. But knowing how SAR might affect your medical device is an important consideration before starting your project.

For end user medical applications, suppliers offer gateway boxes that will convert RS232, RS485 or Ethernet to 802.11 WLAN. These boxes almost always come with FCC certification. For OEM applications where the WLAN interface is integrated into the medical device, suppliers offer WLAN modules that come with FCC Modular approval. This means that the module supplier performed the testing necessary to get FCC approval, allowing medical device manufacturers to use the testing to gain FCC certification for their medical devices.

Conclusion

With proper planning and preparation hospitals and other health-care facilities can easily benefit from medical device integration. By using a step-by-step approach and being aware of the potential integration issues upfront, health-care facilities can integrate ALL of their medical equipment, both legacy and new, into their EHR and EMR solutions.

Appendix A.

This table lists commonly-used RS-232 signals and pin assignments.[7]
Source: http://en.wikipedia.org/wiki/RS-232

Signal			**Origin**		**DB-25 pin**	**DE-9 pin**	**TIA-561 pin**	**Host pin**	**DEC MMJ**
Name	**Typical purpose**	**Abbreviation**	**DTE**	**DCE**					
Data Terminal Ready	OOB control signal: Tells DCE that DTE is ready to be connected.	DTR	●		20	4	3	2	1
Data Carrier Detect	OOB control signal: Tells DTE that DCE is connected to telephone line.	DCD		●	8	1	2	7	6
Data Set Ready	OOB control signal: Tells DTE that DCE is ready to receive commands or data.	DSR		●	6	6	1		
Ring Indicator	OOB control signal: Tells DTE that DCE has detected a ring signal on the telephone line.	RI		●	22	9		-	-
Request To Send	OOB control signal: Tells DCE to prepare to accept data from DTE.	RTS	●		4	7	8	1	-
Clear To Send	OOB control signal: Acknowledges RTS and allows DTE to transmit.	CTS		●	5	8	7	8	-
Transmitted Data	Data signal: Carries data from DTE to DCE.	TxD	●		2	3	6	3	2
Received Data	Data signal: Carries data from DCE to DTE.	RxD		●	3	2	5	6	5
Common Ground		GND	common		7	5	4	4, 5	3, 4
Protective Ground		PG	common		1	-	-	-	-