Thinking about wireless systems? 
Consider these tips from an expert

Are you considering wireless technology for tracking patients, staff, equipment, or supplies?

Expert tips are offered by Rick Hampton, wireless communications manager for Partners Healthcare. The Boston-based network includes Brigham & Women’s Hospital, Massachusetts General, and affiliated facilities.

Many hospitals are weighing decisions about these technologies, which include RTLS (real-time locating system) and/or RFID (radiofrequency identification).

Involve IT, biomed early
Hampton strongly recommends involving your IT and biomedical engineering departments before talking with vendors.

“If you don’t, you might buy a system that violates your organization’s security rules or is incompatible with other systems,” he says. The OR’s plans should be part of a strategic plan for wireless technologies, ideally, for the entire hospital.

One size does not fit all
In a wireless network, all technologies that use it share its bandwidth. Consider how adding a new technology could affect the performance of others using the system.

“There are no one-size-fits-all technologies. Wireless is always a compromise,” Hampton says. “You really need to plan.”

For example, an RFID system designed to have a high degree of accuracy with frequent signals, such as Wi-Fi documentation of patient data, might adversely interact with other systems using Wi-Fi, such as OR voice-over IP phones or video streaming.

Overtaxing the system is more likely in hospitals with lots of applications. Proper planning allows IT and biomedical engineering to install and design the wireless networks from the beginning to support as many systems as possible and avoid redesigning them with each new technology purchased.

Don’t overlook security issues
In most cases, RFID systems don’t transmit sensitive information. But some wireless RFID systems have potential to create a “back door” into a secure network.

“That’s our number one concern—preventing holes in our firewalls,” Hampton says. “Much of RFID came from other industries like retail and manufacturing where security is not nearly as critical.”

RFID systems that use one-way transmission to dedicated receivers are less of a threat than those that transmit using the IT Wi-Fi network. Proprietary RFID systems that use 2-way transmitters “are particularly problematic,” he says, because a hospital doesn’t have the means to detect an attack.

If your facility is audited for compliance with patient privacy laws, regulators will expect to see an audit trail showing the hospitals has determined that such systems are secure.
“That can be difficult if you don’t get documentation from the vendor on how its system meets your security requirements,” he says.

With any wireless RFID system, especially proprietary ones, he says he would expect the manufacturer to provide a risk management analysis of security risks and how they are mitigated. Each organization then has to weigh the risks versus benefits.

**Plan strategically**
Before talking with RFID vendors, define the problems you want to solve. For each problem to be solved, create a use case with a list of requirements, description of work flow, and desired outcomes. Then ask if the new technology is the best approach, Hampton suggests.

“RFID is the latest and greatest solution. It doesn’t mean it’s always the best,” he says.

A variety of technologies are available for determining location and identification of items, each with their strengths and weaknesses.

“You should match the technology to the use case, not the other way around,” he says.

If you want to track mobile equipment, for example, a number of systems are on the market. For temperature monitoring of refrigerators and freezers, an alternative may work just as well because these are not mobile. Uses that require a high degree of accuracy for documentation, such as tracking patient treatments or identifying all equipment used on a particular patient, “turn out to be fairly difficult,” he says.

In selecting a vendor, he adds, be aware that a vendor with hardware that meets your needs may not have software that works well and vice versa. You may need to mix and match.

**Interference**
Under normal circumstances, Hampton says he wouldn’t expect interference to or from an RFID system. Still, the potential exists, and rare incidents have been reported.

There are no standards or certifications that show an RFID system will not cause interference, he notes. There are, however, standards that show medical equipment is manufactured to minimize susceptibility to interference; IEC 60601-1-2 is one such standard.

“Be wary of companies claiming their RFID systems comply with any of these standards; this indicates they generally don’t understand interference and could be of limited help if you do have problems,” Hampton says.

**Don’t expect to trial**
Don’t be surprised if RFID vendors tell you they don’t do prepurchase trials or pilots, Hampton notes. Many vendors now expect the hospital to simply purchase the equipment and install it.

“Doing this means you won’t know until after signing a purchase contract that the system may not work,” he says. If that’s the case, he advises the hospital to include a strong nonperformance clause in the contract.

—Pat Patterson