Network vulnerabilities are putting patient confidentiality and safety—fundamental ethical and legal tenets in healthcare—at risk. As healthcare becomes increasingly intertwined with information technology (IT), hackers, viruses, and system glitches have the potential to disrupt medical devices and undermine the security of
private information. Consider the sensitive information that has been exposed by data breaches alone every year, potentially affecting millions of patients:1,4
- Personal information, including names, dates of birth, Social Security numbers, home addresses, telephone numbers
- Medical records and clinical information, including test results, diagnoses, diagnosis codes, treatments, disability codes, and X-ray and other images
- Financial and insurance information, including bank account, credit card, and insurance numbers

And consider the potential impact of data breaches on patients and their families, a threat that's underscored by the federal government's push for the widespread use of electronic health records. "In the last 14 months, both of my parents have had their health records breached—from different healthcare facilities," says Derek Brost, chief security officer at eProtex, a data security company based in Indianapolis, IN, that specializes in the hidden risks of connected medical devices.

"It's ridiculous how casually some healthcare facilities are handling people's private medical information," Brost says. "And also, oftentimes, that ties to your financial information. My parents are retired. They're in a position where they're starting to get a lot more medical treatment. This could have a big impact on their end-of-life care treatment options if their personal, medical, and financial information was in any way compromised.

Patient confidentiality isn't the only risk. Security breaches of medical technology networks sometimes compromise patient care and safety. If a network or a networked medical device is hit by a security breach, it can take down vital healthcare services, and related business services, along with it. And sinister attacks on portable and implantable medical devices, while hypothetical now, have the potential for increased growth and threats in the future. If the threat follows the trajectory that cybersecurity in other industries has taken, it could ramp up significantly in the not-too-distant future.

Equally alarming, many healthcare organizations "don't know what they don't know" about their susceptibility to security breaches. In fact, many only realize their vulnerability after an incident occurs.

In terms of threats to the functioning of devices, some security experts over the past year have said they have successfully hacked into wireless medical devices, taking control, for example, of insulin pumps. Manufacturers say they take such claims seriously and are ramping up encryption efforts.

'The Threat Landscape'
Several interrelated factors are making medical technology networks more vulnerable both to malicious attacks from hackers around the world and to internal security threats, whether accidental or intentional.

Two major developments over the past year concern security expert Axel Wirth:
1. The increasing prowess and malevolence of attackers. "Overall, what we call the threat landscape is increasing to become more and more sophisticated, or more and more dangerous," says Wirth, national healthcare solutions architect at Symantec Corp., a global software and services company. "Meaning that the bad guys are getting smarter and smarter. The attacks we are seeing are getting more and more targeted, evasive, and difficult to detect." In an article in the January/February 2011 issue of BI&T, Wirth noted that hackers who used to be interested primarily in “making a splash” are now moving “from fame to fortune.” Says Wirth: "Nowadays, the underground economy is into it for financial gains. That’s identity theft, stealing bank and credit card information, stealing corporate information. That also means that rather than making their tactics known and making that big announcement—’ha ha, your computer is infected’—they are now deliberately being evasive and utilizing technologies to keep them from being detected so they can carry out their attacks to the fullest extent."
2. The increasing use of “off-the-shelf” software to power medical technology. More manufacturers are using off-the-shelf operating systems, including Windows, Linux, Unix, and other third-party software. “You look at many of today’s medical devices—an X-ray machine, an MRI scanner, a patient monitor, a medication cabinet, you name it—and you will
THE MAGNITUDE OF THE PROBLEM

How big is this problem? The healthcare industry had some dubious distinctions in 2011 that provide some insights:

• The number of reported security breaches in healthcare increased by 32 percent from 2010 to 2011, according to the Ponemon Institute, a security research group.

• Three of the six most significant data breaches occurred in healthcare, according to the Privacy Rights Clearinghouse, a nonprofit consumer organization that has been tracking data breaches since 2005. These breaches include:
  – Sutter Physician Services and Sutter Medical Foundation, Sacramento, CA—A stolen desktop computer, with data that was password-protected but not encrypted, exposed the records of 4.2 million patients. At least two class-action lawsuits have been filed.
  – Health Net, Rancho Cordova, CA—Nine data servers containing sensitive health information of 1.9 million patients went missing.
  – Tricare Management Activity, Science Applications International Corporation—Backup tapes containing health information from patients at military hospitals were stolen in a car theft, exposing the health and financial information of 5.2 million patients. Four people have filed a $4.9-billion lawsuit on behalf of the patients.

• The healthcare industry is second most vulnerable to data breaches, behind business, as shown in Figure 1.

According to John F. Murray Jr., software compliance expert at the U.S. Food and Drug Administration (FDA), “At the current time, the agency has only received a very small number of cybersecurity-related reports. The FDA continues to encourage the reporting of cybersecurity-related failures in accordance with well-established Medical Device Reporting Regulations.”

find that once they are connected to a network they actually look very similar, if not the same, as a regular desktop, laptop, or server,” Wirth says. “They are vulnerable to the same attacks. They can be infected with the same viruses as other IT systems for which the viruses were actually written.”

Earl Reber, executive director of eProtex, adds a third development:

3. More networked medical devices and more devices that capture electronic protected health information. “Just as it becomes more dangerous to drive as more cars get on the road, we have that same increase in traffic on networks,” Reber says. “Statistically, to give you an idea, one of the first hospitals we performed services in had about 0.7 networked medical devices per hospital bed. Now, we see an average of close to, and in many cases just over, two medical devices per hospital bed. And even at that very first hospital, we tracked it and it’s up to over 1.34 to 1.4 medical devices per bed in the short span of two years, from 2009 to 2011. That’s a significant increase.”

This increase in networked medical equipment means that if there is a hacking incident or other security breach, traffic on the network can slow down and interrupt healthcare services and productivity. Moreover, the increasing use of mobile devices, from smartphones to tablets to portable storage devices, adds complexity to network security in healthcare.

“The risk of patient and/or user harm from connected or networked devices in the healthcare environment will depend on the specific hazard that has occurred—for example, loss,” says Leanne Cordisco, healthcare IT program manager, education services, at GE Healthcare. “The risks are the same for wired and wireless devices, but the causes of those risks vary greatly between the two. Medical devices providing real-time patient data through the network, for either centralized or remote clinical review, are particularly vulnerable to network disruptions, which may interfere with and adversely impact patient care.”

Finally, the risk profile for medical technology is affected by regulations from the U.S. Food and Drug Administration (FDA), the Health Insurance Portability and Accountability Act (HIPAA), and the U.S. Department of Health and Human Services Office of Civil Rights, among others. Whereas hackers and

Figure 1. Security Incidents by Industry. (Source: Open Security Foundation/DataLossdb.org.)
malware—such as computer viruses, worms, Trojans, spyware, and botnets—can move at lightning-fast speed, adaptations to safeguard medical equipment and networks from security breaches can take time.

Taken together, here’s the bottom line: The “bad guys” are more adept at trolling for valuable information they can turn into a profit. Off-the-shelf software can make medical devices and networks easy to prey upon—or harm inadvertently. With more medical technology connected to networks, and more sensitive information collected and dispersed, protection is more difficult—and security breaches can be more severe.

‘Collateral Damage’
The use of off-the-shelf software offers a prime example of the “collateral damage,” in Wirth’s words, that can occur from security breaches. Off-the-shelf software, such as operating systems, browsers, and databases, is becoming more popular because it is familiar to people and thus easier to use, it facilitates connectivity and interoperability, and it is less expensive than developing proprietary software.

“Our data show that 40 to 50% of networked medical devices rely on Windows-based systems, about 30 to 40% percent are based onLinux or Unix systems, and about 10 to 20% percent are still proprietary operating systems written for specific companies or specific devices,” Reber says.

One problem is with software “patches” or updates. Software companies regularly push out patches to protect against the latest malware or other security or software glitches. Business and personal users can install these updates quickly and easily and get on with their work.

Medical technology manufacturers, however, might have to go through an FDA review process before they can give their customers the go-ahead to install the updates to ensure that the update does not impact the safety and functionality of the device. “If I’m a manufacturer, because of that rigorous process, I am challenged to release security patches quickly, I’m more or less behind, depending on the efficiency of my release processes,” Wirth says. “I can’t just say, today is Tuesday, I get a new set of patches from Microsoft and I start distributing them. I have to test them first on my device. I need to make sure those changes to the operating system don’t impact behavior and functionality of the system and then I can tell my customers, ‘Yes, you can now deploy this operating system.’ That means that medical devices, from an operating system patch level, often are months, if not years, behind where the operating system manufacturer is—meaning that there is a huge, gaping security hole.”

That gaping security hole could bring healthcare organizations to their knees. Malware can be introduced into an organization in many ways, Wirth says, be it via mobile data carriers or users’ desktops and laptops. But, because they are connected to the network, they can pass the virus to medical devices that are not as robustly “inoculated” against infection. But, because they are connected to the network, they can pass the virus on to medical devices that are not as robustly “inoculated” against infection.

If a virus spreads to medical equipment, its effect can ripple across entire departments and beyond. Many hospitals, for example, prefer to procure a particular type of medical technology, such as imaging equipment for a catheterization lab, from a single vendor. That vendor keeps all of its equipment on the same patch or configuration level. “As soon as one device in that cath lab gets infected, then the same device in all other labs are at risk of getting infected,” Wirth says. “All of sudden, before you know it, your entire interventional cardiology is shut down.” Other networked medical devices, or other IT equipment that is not up-to-date with patches, can “catch” the spreading virus as well. “You have a virus gone rampant throughout your hospital because it is being spread from medical device to medical device.”

Thus, while an initial virus or other security breach might not target medical equipment, it can result in broad “collateral damage.” Security breaches can impact patient care and safety, if treatment is delayed or diverted, as well as staff morale and productivity. They also can result in financial loss from equipment downtime, which can range from hours to days, or repairs from outside service providers.

Security breaches in healthcare are particularly challenging for another reason. If a business or home computer becomes infected with a virus, the first action for troubleshooting is to disconnect it from the network, and disconnect similar equipment that might be prone to the same virus. But it’s difficult for a

A Federal Warning

Warning of a “significant risk of harm” to patients, a federal advisory board wants medical devices to be reviewed for cybersecurity vulnerabilities before and after they are approved for sale.

The chairman of the Information Security and Privacy Advisory Board said greater oversight is needed because of the proliferation of software-based medical devices that hook up to the Internet. “With increasing connectivity comes greater functionality and manageability, but also increased risks of both unintentional interference and malicious tampering via these communication channels,” wrote Daniel J. Chenok, chairman of the board, in a March 30 letter to Jeffrey Zients, acting director of the U.S. Office of Management and Budget.

Chenok wrote that the board was alarmed by a lack of responsibility for cybersecurity among government agencies. The board made numerous recommendations. Among them, a single entity such as the U.S. Food and Drug Administration (FDA) should take cybersecurity into account “during premarket clearance and approval of devices, and during postmarket surveillance of cybersecurity threat indicators at time of use.”

In addition, the FDA should collaborate with the National Institute of Standards and Technology (NIST) to research cybersecurity features on networked devices that can be enabled by default. “For instance, a medical provider should not have to download new software, such as an antivirus product, to achieve an acceptable baseline of cybersecurity.”

To read the letter, go to: www.aami.org/news/2012/042512_ispab-ltr-to-omb_med_device.pdf
Personal devices are harder to control than devices issued and configured by healthcare organizations, but even hospital-issued devices can never be 100 percent secure.

healthcare facility to disconnect every similar piece of medical equipment, especially if that equipment is essential for patient care or even life support.

Equally troubling is the installation of unauthorized software updates, which eProtex’s Reber and Brost have encountered. Some company representatives will “unofficially” tell customers that they can install software patches without any negative effects.

“A gamma camera is a great example we’ve run across in the field where it was being infected with viruses,” Reber says. “There was a patch that wasn’t applied, and wasn’t authorized to be applied, but the manufacturer’s tactical service rep said to go ahead and put the patch on. As soon as we put the patch on, we found out that a gamma camera uses 22 ports to transmit its information. That patch restricted the operating system to a maximum number of open ports of eight. And so, the gamma camera could no longer transmit data in a timeframe that it could work within, and the camera failed in its operation.” That exposed the patient to radiation without producing a usable image and it slowed down the diagnostic process.

In one case, a computed tomography (CT) scanner in an emergency room became infected with a virus, forcing staff to divert a patient to another department for imaging. “In an emergency department, you’re usually talking about a trauma patient,” Reber says. “You have to divert that patient to a different department and kick other patients off the equipment. That’s a potential patient safety issue.” Another downside to events on equipment like this is that healthcare institutions may not have extra or backup units available.

Such scenarios concern Reber, an attorney, for another reason: the potential liability issues. “My biggest nightmare as an attorney is being the defense attorney for the first time that a patient is misdiagnosed because a medical device either has a virus or, worse yet, had antivirus or other unauthorized software put on it and contributed to a misdiagnosis or a mistreatment,” he says.

Internal Vulnerabilities
While external cybercrime is a real threat, security risks abound inside healthcare organizations as well. Even healthcare organizations with strong protection, through firewalls and other technologies, face internal risks. Points of vulnerability include:

- **Mobile devices**, such as smartphones, laptops, and tablets. The sheer number of mobile devices in use in healthcare, by healthcare staff, patients, and visitors alike, is challenging healthcare organizations to provide a robust, wireless infrastructure to support them, Brost says.

Physicians and other healthcare staff like to access their e-mail and patient records from their homes or on the road—and in their facilities. “Potential risks associated with smartphones and tablet computers such as iPads are increasing with each new application and product generation that is released,” Cordisco says. “No longer can these devices be viewed as a secondary form of display or data system. Rather, clinicians are relying upon them as the primary information source with increasing frequency and, as such, the risks to patient care can be greater if the manufacturer does not take this expanded use into consideration.”

For example, people can inadvertently send or receive files from their personal e-mail accounts, which are easier to breach than their institutional accounts. Plus, these devices are easily lost or stolen. Any files on the device, and automated login and password information to access information, can be retrieved and potentially abused.

Legal and financial issues associated with data breaches like these concern Kenneth Maddock, vice president of healthcare technology management and telecommunications services at Baylor Health Care System. “We have to be concerned about this because as an organization we’re going to be evaluated on it from a legal and ethical standpoint. We had a device stolen, and fortunately we were able to wipe the hard drive clean quickly. But you still have to report it in a specific amount of time and take steps such as offering those affected credit counseling. You can get enormous fines if it is deemed that you aren’t doing enough.
And above all you want to protect patient information because it’s the right thing to do."

As the “bring your own device” trend reaches healthcare, this vulnerability will increase. Personal devices are harder to control than devices issued and configured by healthcare organizations, but even hospital-issued devices can never be 100 percent secure. “Any mobile device that can be used outside of the hospital to access patient records—if not properly managed and protected—can lead to a privacy breach,” Wirth says.

Right now, Windows- and Android-based mobiles with open architectures are easier to attack, and incidents against these devices are on the rise. Apple’s iOS operating system for iPads and iPhones is “relatively well architected and relatively safe,” Wirth says. But he cautions that hackers likely are trying to find ways to change that.

“Lots of times, we’ve seen clinicians bring in devices that they want to use that IT hasn’t reviewed or approved yet,” Brost adds. “The concern I have is around data security—if a clinician loses that device or forgets it or he forgets which e-mail account he’s using. He meant to send the e-mail over his hospital account and selected his personal account. These are creating breaches that just weren’t a possibility before because you had to physically sit down at a hospital on a computer, physically access the database and patient records. You didn’t have remote access and portable computing access. The change has happened faster than the security and privacy offices have been able to keep up with.”

- **Portable media**, such as CDs and universal serial bus (USB) sticks. Wirth says he’s seen many instances of “a service technician—whether from a manufacturer, a third party, or a biomedical engineering department—walking around with a USB stick and installing a legitimate software patch onto a medical device. The USB stick may carry a payload and the payload may be a virus.” It’s hard to verify where these devices have been, and whether they have picked up a virus somewhere.
- **“Stealth” devices.** Sometimes healthcare staff or departments bypass established procure-

---

**Stephens International Recruiting Inc.**

“Connecting Quality People, Quality Service”

Experienced executive health care recruitment and placement services specializing in clinical engineering / biomedical equipment services positions nationwide, to include Military/OEM-trained professionals, with specific emphasis on the following positions:

- Biomedical Equipment Technicians (BMETs)
- Radiology/Imaging/Nuclear Technicians & Managers
- Equipment Field Service Technicians / Engineers
- Directors / Managers / Executives for Above Specialties, Regional and National

Contact us for alternative staffing solutions with our Temp-to-Perm or Temporary/Contract Biomedical Staffing Services. We also provide recruitment and placement services for all Executive/Management, Clinical, and Professional health care positions nationwide.

**EXECUTIVE HEALTH CARE RECRUITMENT AND PLACEMENT SERVICES**

*Contact: Tim Hopkins or Cindy Stephens*

Toll-free: (888) 785-2638 (BMET); Direct: (870) 431-5485

E-mail: info@BMETs-USA.com

www.BMETS-USA.com
Some healthcare organizations are remiss when they replace old equipment, simply chucking computers into the dumpster without wiping their hard drives clean, for example.

- **Outside—in attacks.** “Where we see some issues is what I would call an outside—in attack—people using computers to go to Facebook, to go to file-sharing sites, to send and receive personal e-mails,” Wirth says. And that increases the risk of something bad coming in as a payload to that personal traffic. That doesn’t mean these people are going to bad websites. It’s just that the more websites people go to, the higher the risk that the website may be temporarily infected with a virus, which then comes in.”

- **Inappropriate staff access to information.** “Curious” staff members have been known to examine the medical records of friends, neighbors, and family members who are not in their care. Both clinicians who have access to this data, and other staff members who don’t, have been caught in this act. Sometimes this inappropriate access goes beyond snooping to fraudulent use of patients’ Social Security or banking information, for example, for financial gain.

- **Inappropriate disposal of electronic devices and records.** Some healthcare organizations are remiss when they replace old equipment, simply chucking computers into the dumpster without wiping their hard drives clean.

for example. Patient data and other sensitive information can be recovered and used for illicit purposes.

The Open Security Foundation’s datalossdb.org website tracks incidents of data breaches resulting from vulnerabilities like these in healthcare and other industries. Figure 2 shows the breakdown of security incidents by vector.⁸

**Scary Scenarios**

Potential compromises of patient confidentiality, care, and safety, the collateral damage that can result from data breaches, are disturbing. Deliberately harming patients on networked or wireless medical devices would be far worse.

That possibility rattles healthcare security experts. Medtronic in 2011 announced it would conduct an “in-depth risk/benefit analysis” after reports that one of the company’s insulin pumps is vulnerable to hackers.⁷ The fear is that hackers could gain remote access to the pump and reprogram it to deliver a potentially lethal dose of insulin.

Researchers at Massachusetts Institute of Technology and the University of Massachusetts, Amherst, meanwhile, have demonstrated that it is possible to hack into wireless, implantable medical devices, such as pacemakers, heart defibrillators, cochlear implants, and neurostimulators, and reprogram them in ways that could harm patients.⁸

Wirth emphasizes that these are “hypothetical” scenarios. “This has all occurred in a lab setting—but repeatedly, and for different kinds of devices,” he says. “This could be a problem in the future in a riskier scenario because of where those devices are, inside the patient, and what function they have, which is typically sustaining or at least life supporting. If you think about it, it’s really scary.”

Baylor’s Maddock echoes that thought. While there is no evidence that these kinds of adverse events are occurring, healthcare technology managers need to keep them on their radar screen.

“The real problem is we just don’t know what we don’t know,” Maddock says. “Anytime you add a technology you at least have to start thinking about the types of potential attacks. While the primary responsibility is on the manufacturers to harden the devices against potential attack, we do have a role. This is a new and evolving area of technology and I’m not sure that those of us

---

**Figure 2.** Security Incidents by Vector, 2011. (Source: Open Security Foundation/DataLossdb.org.)
Expert Advice

HTM Professionals, Manufacturers Have Key Roles to Play

In an e-mail interview, Leanne Cordisco, healthcare IT program manager, education services, with GE Healthcare, answered questions about security and healthcare technology.

What are healthcare facilities, manufacturers, and regulators doing to mitigate risk? What considerations are manufacturers taking into account in the design and development of medical devices?

The standard ANSI/AAMI/ISO 14971 directs that medical device manufacturers (MDMs) follow a thorough risk-management process during product development and on an ongoing basis after the devices are placed on the market (i.e., product surveillance). In this process, all aspects of the device’s operation for its intended use are evaluated. When a risk is identified, the MDM typically takes measures to reduce or eliminate the risk through product design and labeling. Factors taken into consideration by manufacturers include advances in medical technology, clinical environments, and use scenarios as well as post-market data during the design and development of medical devices.

In addition to benefits derived from risk management activities performed by MDMs, there is also significant value for healthcare delivery organizations (HDOs) to perform their own risk management, in the context of their planned use of the medical device. This is especially true for medical devices that an HDO connects to its IT networks, for example when building more complex systems customized to its specific needs. The need for such risk management by HDOs, with the support of MDMs and vendors of other IT equipment, is addressed by the new standard ANSI/AAMI/IEC 80001-1. This is an important tool providing a framework for HDOs to manage their networked devices. An important feature of ISO/IEC 80001-1 is the provision of “accompanying documents,” providing essential information for the medical device to be incorporated onto a shared network.

What role do healthcare technology management professionals play in safeguarding the security of medical devices in this environment?

Clinical engineers and biomedics are able to contribute to safeguarding the security of medical devices through their involvement in the selection process of the medical device, as well as during implementation planning, launch, and ongoing maintenance support of the medical device. Clinical engineers may also share the duties associated with the role of the medical IT network risk manager as addressed in the 80001-1 standard.

The medical IT network risk manager oversees the entire risk management process and in the evaluation phase and interfaces with vendors to obtain important security and risk management information, such as the Manufacturer Disclosure Statement for Medical Device Security (MDS2). The intent of the MDS2 is to supply healthcare providers with important information that can assist them in assessing the vulnerability and risks associated with electronic Protected Health Information (ePHI) transmitted or maintained by medical devices. This standardized form, jointly developed by Healthcare Information and Management Systems Society (HIMSS) and National Electrical Manufacturers Association (NEMA), facilitates the HDOs’ review of the large volume of security-related information supplied by MDMs and IT vendors.

Clinical engineers should be available during the go-live stage to ensure that the new device works as intended and does not create new problems in the networks. They can also facilitate processes that require coordination between clinicians and IT or biomedical engineering, especially in cases where networked functionality might be disrupted such as during a network upgrade. And last but not least, clinical engineers should manage equipment maintenance, updates, and patches, to minimize the potential of any risk during these processes.
A Hacker Makes Waves

Security experts say wireless medical devices can be particularly vulnerable to hackers.

In one incident that received widespread media attention last year, Jay Radcliffe, a diabetic and cybersecurity expert, announced at the Black Hat security conference in Las Vegas last summer that he had hacked into his own insulin pump. According to news reports at the time, he took to the stage to demonstrate how he did it, telling attendees he was able to control his pump remotely, altering the critical dosage of insulin.

Medtronic, the maker of that pump, described the risk posed by hackers as “extremely low,” but also said it was redoubling its efforts to develop and use the best encryption and security technologies with its products.

“Medtronic takes patient safety and device security very seriously, and we appreciate the security community bringing new information on the possibility of manipulating or hacking our insulin pumps,” Medtronic said last October. “We have been increasing our focus on the prevention of tampering with our products.”

Some members of Congress, meanwhile, have called on the Federal Communications Commission to review its approach to the regulation of wireless medical devices to ensure that they are “safe, reliable, and secure.”

Managing the Risk

As healthcare organizations integrate more networked medical equipment and implement electronic medical records, managing security and safety risks will become increasingly important.

Robust risk management is the first line of defense, a point recognized by various stakeholders with the development of ANSI/AAMI/IEC 80001-1, a standard which deals with IT networks incorporating medical devices.

“Risk management is an ongoing process for all networked devices used in healthcare, whether as a ‘traditional’ medical device that uses stand-alone software or as a medical device with extended connectivity including Internet access, such as tablet computers and smartphones,” Cordisco says. “Risk management starts long before the device is put on the market and continues until it is decommissioned. Part of risk management includes appropriate protections for medical devices with web access against possible breaches of device security.”

Risk management should consider the risks to patient safety and data security. Both are important. Healthcare organizations might want to supplement their regular risk management activities with these steps recommended by security experts:

- **Conduct a risk audit.** Start by targeting five or 10 different networked medical devices. Analyze the risk profile of these devices using HIPAA security rules for administrative, technical, and physical safeguards. “Usually when we do a HIPAA audit, we average eight or nine findings per medical device,” Brost says. Risk audits can be conducted in-house or by third-party service providers.

- **Develop a risk remediation process.** Bring together a team of people, including CE, IT, and if necessary, facilities experts. Work together to mitigate the risks associated with that first set of devices, using HIPAA, FDA and Joint Commission guidance. “Even within the same healthcare systems, different facilities want to tackle their risks differently,” Brost says. “They may have different tolerance for risk. They may know they have a risk and be willing to accept it, which is fine, as long as they make a dedicated, informed decision.”

- **Make risk remediation an iterative process.** Develop a plan for auditing every medical device within the healthcare system. This will take time and, possibly, funding that needs to be built into budgets. But if you ever face an external audit [e.g., HIPAA, Joint Commission, or Office of Civil Rights audits], it’s important to show that you have a program, policies, and procedures in place for making incremental improvements over time—and a “road map or strategy even if the destination is multiple years off because of resource constraints,” Brost says.

- **Look for “low-hanging fruit.”** There are simple, low-cost and no-cost measures healthcare organizations can make to improve safety and security. Install a lock on the door to prevent unauthorized access to medical equipment and patient information. Turn computer monitors away from prying views. Erase information before discarding obsolete computers and portable digital media. And, for paper records, use a shredder.

- **Consider technology solutions.** Think about e-mail filtering and virus checking, URL filtering, and automated tools to control staff access to potentially harmful websites. Enforce user passwords and password strengths, and consider strong authentication, such as biometrics, to ensure that only people who are authorized to access specific information can do so. Encrypt data on devices and in transit. Separate organizational data from personal data, and organizational e-mail from personal e-mail. Enforce security and privacy controls on mobile devices, whether hospital-issued or personal—and make sure you can wipe clean lost or stolen devices remotely and quickly. Consider adding layers of security to mobile technology by segregating it, with tighter access controls, on the network infrastructure.

- **Explore data-mining tools.** Data-mining tools developed by clinical informatics specialists make it possible to detect whether inappropriate access to healthcare databases is occurring, either from outside hackers or internal staff members.

- **Educate.** Redouble efforts to educate employees about safe and secure use of medical technology networks and mobile devices.

- **Foster better communication and working relationships between manufacturers, CE, and IT.** Make sure the health technology
management team considers the entire ecosystem of networked technology when new devices are installed, Maddock recommends. Adding patient monitors to a network, for example, can affect other databases and equipment. Network security should be verified before the hospital takes ownership of the equipment. And make sure that CE and IT professionals are in the loop when changes, including software updates, are made to medical devices and networks.

• **Keep up with the changing threat landscape.**
  Among the organizations focused on this issue are:
  - The Clinical Engineering–IT Community (CEIT, http://ceitcollaboration.org)—an initiative of AAMI, the American College of Clinical Engineering (ACCE) and the Healthcare Information and Management Systems Society (HIMSS)
  - IHE (www.ihe.net/)
  - Medical Device “Plug and Play” Interoperability Program (MDPnP™, www.mdpnp.org/)
  - Finally, a special caution: Smaller healthcare facilities and doctors’ offices are especially vulnerable to medical technology security risks. These facilities typically do not have a dedicated IT or health technology management staff to safeguard patient data or medical devices. And they are easier targets of physical break-ins and thefts.

**References**


