The last 30 years have witnessed the transformation of medical devices, with personal computers, networks, and application software being incorporated into traditional embedded-system medical devices. Bringing information technology (IT) to the medical device industry enabled new features such as remote surveillance, automated diagnostic report generation, cross-patient data analysis, and much more. Increasingly, medical devices are becoming information appliances on enterprise networks.

So far, the front end of medical device systems, the embedded-system device, remains mostly unchanged. Yet, features and data continue to stream to this new computerized back end of medical device systems. As a consequence of this transformation, the front end is shrinking down to the essence of the medical device, with front-end electronics for physiological along with other sensors and essential therapy delivery components. For some medical devices, the user interface is moving to the enterprise network and running on personal computers, tablets, and smartphones.

Healthcare IT also has transformed. To date, the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 unleashed almost $35 billion to incentivize healthcare providers to adopt electronic health records (EHRs). Hospitals adopted the technology rapidly. More than 95% of U.S. hospitals bought and implemented government-certified EHRs as of today. This dramatic increase in healthcare delivery automation is transforming medical devices into information appliances.

The transformation of healthcare technology management and healthcare IT left many people a little shell shocked. The rush to meet the regulation’s time frame to implement EHRs put most providers in a position where it was all they could do to hold on to existing organizational structures and management processes, instead of evolving governance and policy to accommodate the adoption of these new technologies. Today, the industry understands how complex and resource intensive it is to implement a major information system like an EHR.

With most of the HITECH Act cash incentives already paid out to providers, it’s time to re-evaluate the industry’s response to these changes and work to fill the gaps that grew between how we managed things before these transformations occurred and the needs of today’s technologies. Manufacturers and provider organizations need related but different changes.

**Product Architecture**

Product architecture and data security are the biggest challenges for medical device manufacturers. There is often a market for new and innovative sensor or therapy delivery technologies. However, due to the maturity of the medical device industry, these types of innovations are more difficult and expensive to realize than in the past. Consequently, much of today’s medical device product development revolves around workflow automation in support of the essential characteristics of the medical device.

Leveraging off-the-shelf IT components results in better features, shorter time to market, and lower development costs compared with building these features into the embedded system device. The challenge lies in the differences between best practices for product development in the general purpose computing platform world and those for embedded-system medical devices. This transition requires changes such as new infrastructure (e.g., network and systems integration test labs) and technical core competencies. Features best suited to general-purpose computing platform architectures include data acquisition and analytics, alarm notification, user interface, and components for enabling mobility.

**Data Security**

Both manufacturers and hospitals lag behind the curve of medical device data security. Manufacturer best practice remains focused on designing the product first and then considering data security as an add-on. Just as it is less expensive to fix design flaws in the design phase rather than in production, data security is more effective and less expensive when designed into a product from
the beginning. Despite the best data security efforts, vulnerabilities will be found and must be eliminated. Manufacturers must be able to test and distribute to customers their own security vulnerability software patches and patches from third-party suppliers in a timely fashion.

While some providers use the HIMSS/NEMA MDS (Healthcare Information and Management System Society/National Electrical Manufacturers Association Manufacturer Disclosure Statement for Medical Device Security) form2 or other tools to gather data security information from manufacturers, every hospital must identify vulnerable devices and protect them with effective configuration management, firewalls, network segmentation, and the timely application of software patches. Hospitals also need to provide intrusion detection and incident response tailored to medical devices.

Hospital Policy and Procedure Safety Gaps
The transformation of medical devices into information appliances affects provider organizations as much as manufacturers. Many people in biomed/clinical engineering (CE) together with IT work hard to ensure patient safety and the proper operation of medical device systems. However, the written policies and procedures fail to pass basic quality system criteria for either department in most hospitals.

The responsibilities for medical device systems are typically divided between IT and biomed/CE departments. The division between the portion of medical device systems supported by IT versus biomed/CE is somewhat arbitrary. This division often lacks an explicit, formal policy that would provide a documented process to coordinate the two departments, which would ensure the proper deployment, maintenance, and repair of systems. Instead, the coordination of work effort is handled informally.

Device inventories are another example of divided responsibilities between IT and biomed. The general-purpose computing platform items of medical device systems end up in the IT inventory while the embedded system devices end up in the biomed/CE inventory. Managing large and complex systems in one system is a challenge. Doing so with two separate inventories—each in a different department—is problematic. Very few hospitals conduct audits to validate that these two inventories are correct. The audits ensure that all items are accounted for in one of the inventories and checks that items are not recorded in both inventories and potentially “managed” by two departments at the same time.

Managing large and complex systems in one system is a challenge. Doing so with two separate inventories—each in a different department—is problematic.

IT department policies and procedures often include risk management as it pertains to privacy and data security. Patient safety is not a focus of IT department risk management policies despite research showing that EHR implementation errors can result in sentinel events as well as the safety risks associated with medical device systems.

The patient safety risk management gap is typically not much better in the biomed/CE department, where risk management is often limited to determining optimal preventive maintenance and calibration and inspection periods, rather than patient safety. The International Electrotechnical Commission (IEC) standard IEC 80001, Application of risk management for IT-networks incorporating medical devices,3 was created to foster patient safety-oriented risk management for medical device systems, but few hospitals have adopted it.

The IT department retains a rich set of tools for network device discovery, configuration management, and change control. Typical IT tools work poorly with most medical device systems because they lack basic IT features such as dynamic host control protocol, network time protocol, or simple network management protocol. Establishing comparable capabilities for medical device systems as conventional IT systems requires specialized tools and additional effort. As a result, many hospitals lack complete documentation on medical device system configurations.

Many biomed/CE departments lack explicit
change-management policies, and IT department change-management policies often lack any formal consideration of patient safety. The objective evidence of a complete change-management process in most hospitals is highly abbreviated and limited to the completion of one or two fill-in-the-blank forms. While this approach is fine for upgrading print servers, changes that affect medical devices should receive a more rigorous process, including a patient safety–oriented risk assessment.

Organizational Transformations
The confluence of changes to medical devices and the state of EHR adoption exert pressure for organizational change. Some hospitals changed their reporting structures by moving the biomed/CE department under IT. Politically, this is a big move. But it results in few real changes that might address the shortcomings noted above.

More substantive changes that are starting to see adoption include a combined service model, which combines IT and medical device requests. Once IT and biomed/CE share a common trouble ticket system, the next logical step is establishing a shared inventory or asset management system. This step is complicated by the fact that an asset management system must support the characteristics of medical devices that are not shared by information technology (e.g., safety inspections, calibration, preventive maintenance). Typical IT asset management systems also provide network device discovery and configuration management. As noted above, current limitations in medical device systems necessitate additional features and/or manual tasks to effectively support medical devices.

Once a core set of tools are used to manage the shared IT infrastructure and all the attached components (including medical device systems), the lack of a complete and shared set of policies and procedures becomes all the more obvious. From a quality system perspective, a strong case can be made to use one set of policies and procedures for risk management, configuration management, and change control that apply to both IT and biomed/CE departments. This, combined with required objective evidence, would provide the formal framework for the solid work presently done informally between IT and biomed/CE departments.

References
