As medical devices change, the processes used to manage them should likewise change. That's the driving concept behind this year's winning submission from Methodist Hospital of Southern California.

In hospitals everywhere, traditional stand-alone medical devices are giving way to networked, software-driven devices and systems. The Biomedical Engineering Team at Methodist Hospital of Southern California recognized that along with exciting new benefits, these devices bring a new generation of risks. Thus, the team set about reinventing the facility's medical device inspection and preventive maintenance processes. Their objective was to proactively manage the risks associated with today's IT-based medical devices.

Devices that store and process patient information electronically, that integrate into the hospital network, and that can be accessed remotely have different vulnerabilities than traditional, stand-alone devices. Thus, effective management of such devices, the team reasoned, would require identifying those vulnerabilities — particularly those related to the availability and integrity of medical data and the security of a patient's protected health information (PHI) — and implementing a program to manage the risks.

The team's solution was to implement the Integrated Systems Management (ISM) program developed by Renovo Solutions LLC. The ISM program, which is a component of a biomedical engineering management system called RenovoLive, involves new processes and procedures both for incoming medical device inspections and for the ongoing management of the device throughout its useful life.

With the ISM program, incoming inspections now include an assessment of how the device handles data in addition to verifying the operation and safety of the device. This involves factors that could affect compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The HIPAA Security Rule outlines provisions for ensuring the confidentiality, integrity, and availability of protected health information that is transferred or held in electronic form — referred to as ePHI.
A key component of these incoming inspections is the completion of a Security Assessment form. The form includes 57 questions to help assess the risks associated with a particular device. It focuses on the information systems used to integrate the medical devices, along with the controls, policies, and procedures that affect the confidentiality, integrity, and availability of ePHI that is stored within or transmitted by these devices or systems. This Security Assessment helps the team identify risks and take corrective actions or steps to mitigate the risks as appropriate.

Preventive maintenance procedures likewise have been reinvented to address cybersecurity and incorporate activities associated with the ISM program. Activities include: verifying virus protection, applying vendor-approved patches, managing hardware (e.g., servers, workstations), facilitating disaster recovery (e.g., backups, hard drive ghosting), implementing data security measures, and enforcing policies and procedures.

The RenovoLive software is interfaced to the Methodist Hospital Network through a Client Services Module (CSM). The CSM is a set of Windows services that runs on the hospital’s network and is used to capture information on a regular basis, as well as on request from the users’ network. Notably, this configuration allows for continuous monitoring and updating of medical devices and systems. For example, a polling feature remotely captures status and configuration settings of networked medical devices. Information captured includes hardware devices present, the software version and service packs on those devices, antivirus software information, and number of errors within the last 24 hours.

Other components of the ISM program include the review of medical device software agreements (e.g., to clarify the organization’s responsibilities with respect to cybersecurity) and the appointment of a system administrator. This person acts as a liaison between the biomedical engineering and IT departments and is involved in capital acquisition purchases to ensure that the devices purchased are network-compatible, have well-documented security features, and can be safely configured on the network.

**BEST PRACTICES**

Methodist Hospital’s ISM program establishes a well-rounded cybersecurity program, proactively and continually addressing the risks related to the availability and integrity of medical data and the security of private patient information on networked and software-driven medical devices and systems.

In ECRI Institute’s estimation, many facilities have not yet made substantive progress in this area. Thus, the Methodist Hospital program provides a good example for hospitals to follow.

For more information about the award and the other finalists or to submit an application for next year’s award, visit www.ecri.org/hdaward. Learn more about Methodist Hospital of Southern California at www.methodisthospital.org.