Managing devices and systems on the information technology network and integrating data into electronic health records (EHRs) were the top two medical device–related challenges facing healthcare technology management (HTM) professionals, according to the results of a recent survey commissioned by AAMI.

According to survey participants (n = 195 hospitals), the top 10 medical device issues (rated as “challenging” or “extremely challenging”) were as follows:

1. Managing devices and systems on the IT network (e.g., connectivity, responsibilities): 62%
2. Integrating data into electronic health records: 52%
3. Infusion pump systems: 44%
4. Cybersecurity of devices/systems: 43%
5. Device incident reporting/investigations: 33%
6. Managing recalls: 36%
7. Spectrum/wireless management: 30%
8. Battery management: 30%
9. Endoscopy management: 29%
10. Nonhospital-owned devices brought in by patients: 28%

The majority of the respondents (78.5%) reported working in hospitals, while 11% worked for an independent service organization. About two-thirds (67%) of participants described their organization as general/medical surgical, with 16% stating that they worked in an integrated delivery network/system. Most respondents fell within the 45- to 54-year (43%) and 55- to 64-year (30%) age groups.

The top challenges reported in the 2014 survey reflected those seen in previous years, indicating that these are complex, long-term issues that evade easy solutions. Many of the problems, such as managing the interconnectivity of devices on the IT network, underscore the need for systems-level solutions. Technology may be evolving ever faster, but many experts in healthcare believe its advancements will never be fully leveraged until proprietary interests are overcome in favor of interoperable solutions—with the ultimate goal being improved patient care.

Beyond the question of device challenges, survey respondents were also asked to consider other issues related to the purchase and use of technology in their hospital. One of the most striking answers came in response to the question of the biggest mistake made by hospitals when purchasing new technology. Sixty-seven percent identified a failure to include all relevant staff in the purchasing decision as the single biggest mistake, and 35% said their hospital erred by basing the decision solely on price.

BJ&T talked with several AAMI members, asking them to share their top device-related challenges. One theme that emerged was that entrenched ways of thinking and working are stifling progress. For change to occur, healthcare needs to revise its “siloe
The Question of Service Manuals

While not a medical device challenge per se, the difficulty in obtaining service manuals was identified by many survey respondents as a concern. In fact, the question of access to service manuals has been a long-standing issue in the HTM community, with many professionals saying device manufacturers make it difficult, if not impossible, to obtain service information. Manufacturers say they have safety and liability issues to consider when it comes to how repairs are performed and by whom. AAMI has a webpage dedicated to the question of device supportability and service manual resources at www.aami.org/htmconnect/serviceability.html.

Across all industries, it seems as if we are seeing breaches in personal data every couple weeks. Much of the wireless communication among medical devices is to carry patient information, and so it’s very important that it’s secured against potential attackers.

Chris Alexander, a certified biomedical equipment technician at Maryview Medical Center in Portsmouth, VA, spoke of the challenges his team is facing in testing its EHR system. “We need a systems-level approach for testing the data flow through our EHR system, from the patient monitor all the way through to the patient EHR,” he said. “The challenge stems from the fact that we are unable to modify the system so that we can run a test patient through. We need patient-simulator capabilities on the EHR side. That simulated-patient would need to have a dummy patient ID. And any time that ID is called up, no billing would be generated. That’s the problem: having a test patient that is not tied in with billing codes. The software hasn’t been written to accomplish this.”

“Now that we’re integrating everything, we need an overall system. A test patient to run a simulated vital signs on would be invaluable. It would allow us to train nurses and to check the EHR system following repairs,” added Alexander.

Many of the problems Alexander discussed stemmed from the fact that a mix of in-house (e.g., the IT department) and third-party (e.g., the biomedical department, EHR system) entities exist within his hospital. Bridging the gaps among these forces will be essential to overcoming the challenges they face in testing and troubleshooting issues related to their EHR system. He suggested that one individual or group within the hospital with the authority to oversee the continuity of challenges from a systems-level perspective could serve as an ambassador for fostering collaboration.

David Surber, vice president of medical devices for the TÜV Rheinland Group and based in Pleasanton, CA, has a bird’s-eye view of the challenges facing healthcare. His organization works with thousands of medical device manufacturers worldwide, as well as engages several hospitals on the challenges they are facing related to the rise in use of wireless technology. He is seeing both manufacturers and hospitals wrestle with cybersecurity issues.

“In addition to making sure that their networks remain functioning, hospitals also need to perform extensive testing when any new device is added to the network, in order to ensure that the device is not going to bring harm to patients and affect other equipment,” said Surber. “Ideally, the security testing or assessment should be performed by the manufacturer or a third party like TÜV, before the device is delivered to the healthcare organization.”

“The main problem is the introduction of additional portals for malicious attackers to access a hospital’s network,” he said. “We are seeing a dual threat. The first is regarding functional operations of devices. For example, a heart monitor on a hospital network might pick up malware from a neighboring device and start to give incorrect readings. If that monitor is indicating a heart rate that’s different from the patient’s actual heart rate, that could be a real health hazard for the patient.”

“The second threat is related to patient data,” continued Surber. “Across all industries, it seems as if we are seeing breaches in personal data every couple weeks. Much of the wireless communication among medical devices is to carry patient information, and so it’s very important that it’s secured against potential attackers. Hospitals are having to ensure that patient data, in compliance with HIPAA [Health Insurance Portability and Accountability Act], remain secure.”

Anita J. Medlin, a biomedical equipment technician at Johnson City Medical Center in Johnson City, TN, sees similar problems when new devices are incorporated into her hospital’s network. She believes that manufacturers should play a stronger role in troubleshooting these problems from the start. “When an organization purchases wireless and networked devices, the manufacturers should provide a more thorough security and vulnerability assessment of the buyer’s information technology infrastructure, in order to reduce any software issues.
Number of licensed beds in your individual facility (n = 195)

Which of the following best describes your work setting (n = 195)?

How is the healthcare technology management/clinical engineering program managed in your organization (n = 195)?

By whom are you employed (n = 195)?

Which description most closely matches your organization (n = 195)?

Noteworthy challenges that didn’t make the top 10 list

Chemical/biological hazards and occupational safety
Computed tomography repair and preventive maintenance
Wireless technologies (smartphones, etc.) brought in by patients
Magnetic resonance environment challenges:
Dialysis equipment maintenance
Garbage data in gives you garbage data out. If it's not set up correctly, it's not going to produce good results.

— Julian Kelly, RN, BSN, CNOR, manager of the Central Sterile Department at Baptist Health in Jacksonville, FL

Single greatest challenge for your hospital in managing medical devices and systems on the IT network

1. Determining/assigning responsibilities across departments: 22%
2. Convincing the C-suite and other departments that the HTM department needs to be involved early in all decisions: 12.8%
3. Making sound purchasing decisions on devices and systems: 12.3%
4. Reconciling device and systems connections and communication: 10.3%
5. Proprietary software in devices: 8.2%

 Biggest mistakes made by organizations when investing in new technology

1. Not including all relevant staff in decisions: 67%
2. Basing the decision solely on price: 35%
3. Not investigating the “cost of ownership” thoroughly enough: 32%
4. Not doing a proper technology assessment upfront: 31%
5. Making purchase decisions based on the preference of a single clinician: 26%

that could present themselves during install,” she said. “This also would ensure the best security for patient EHRs.”

Tops on Medlin’s wish list is having more information at her fingertips. “Manufacturers are not providing enough formal information in the technical service manuals for technicians to utilize during troubleshooting procedures, which can cause delays during the repair both in time and quality of the repairs,” she said.

Having reliable tracking data for the sterilization process was a top challenge identified by Julian Kelly, RN, BSN, CNOR, manager of the Central Sterile Department at Baptist Health in Jacksonville, FL. “Central sterile services departments need better instrument-tracking systems,” he said. “When an instrument arrives on the decontamination side of Central Sterile, an electronic IFU [instructions for use] would identify the instrument and how the manufacturer recommends reprocessing. Instrument tracking systems can document that all parameters were met in the washer-disinfector. On the clean side, a tracking system can document that the set is complete and, in the sterilizer, that the correct temperature and exposure were achieved, the correct dry time was reached, and that you did not exceed or fall short of any manufacturer recommendation. Then, when I get a set into the operating room, and I scan in that device, I know that every parameter has been met.”

Kelly also noted the great importance of programming such systems correctly. “Garbage data in gives you garbage data out. If it’s not set up correctly, it’s not going to produce good results,” he said.
New Edition!

BMET Study Guide

Preparing for Certification And Sharpening Your Skills

The updated and expanded 2012 BMET Study Guide tests your knowledge of six key areas:

- Anatomy & Physiology
- Medical Equipment Function & Operation
- Safety in Healthcare Facilities
- Medical Equipment Problem Solving
- Electronics & Electrical Fundamentals
- Information systems technology

The CD features 574 interactive questions and answers—each with a detailed explanation—and nearly 200 new and revised questions.

If you manage healthcare technology, or supervise people who do, this educational tool is for you!

Order code: SGCD
List $165 / AAMI member $99

To order call +1-877-249-8226 or visit www.aami.org/publications/books/bmetcd.html

A Special Thanks to the Sponsors of this CD:
ARAMARK Healthcare Technologies, CREST Services, and Stephens International Recruiting Inc.