If you have ever doubted whether all that electronic data zipping around your facility is truly secure from prying eyes, you have good reason to be concerned.

According to one recent analysis of U.S. Department of Health and Human Services (HHS) data,\(^1\) 804 major healthcare facility breaches (each involving more than 500 individuals) affecting more than 29.2 million patient records were reported to HHS between August 2009 and December 2013. In 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act, which requires protected health information (PHI) breach reporting, went into effect.

In 2013 alone, almost 71 million patient health records were breached—a 138% increase over 2012. The single largest incident in 2013 involved the breach of more than 4 million patient records.

That last breach, like 83% of 2013 breaches, resulted from theft—in this case when four unencrypted laptops containing patient names, birthdates, and Social Security numbers, as well as diagnoses information, medical record numbers and service codes, and health insurance information, were stolen from the Downers Grove, IL–based Advocate Medical Group. Reported cases of hacking, on the other hand, were rare, accounting for just 12 breaches. Still, the analysis, which was conducted by an information technology (IT) security firm called Redspin, predicts that may soon change, noting that “the threat from malicious outsiders—hackers—has the potential to wreak havoc on the healthcare industry,” and that personal health records “are high value targets for cybercriminals as they can be exploited for identity theft, insurance fraud,
stolen prescriptions, and dangerous hoaxes,” as well as credit card information. Hacking attacks, the firm concludes, “are likely to increase in frequency over the next few years.”

Other analyses support the one conducted by Redspin and lay out the potential consequences for healthcare facilities. A 2014 industry forecast report by the global information services group Experian, for example, predicts the cyberthreat landscape is bound to get worse. The report says that the “sheer size” of the healthcare system, especially as more people participate, makes it vulnerable. “It’s clear that the industry, from local physicians to large hospital networks, provides an expanded attack surface for breaches,” the report says. New data breach and privacy requirements under the Health Insurance Portability and Accountability Act (HIPAA) Omnibus Rule, meanwhile, mean that the reporting of such breaches will increase even more, so that among all of the industries that collect consumers’ private information, healthcare “is likely to make the most breach headlines in 2014.”

Adding to this chorus of concern is the 2014 “cyberthreat report” by the SANS Institute, which calls the data it examined “alarming,” and notes that “reports of breaches against healthcare organizations, large and small, continue to rise—as do the regulatory fines they are facing for the exposure of protected patient data.” The Ponemon Institute’s latest “Benchmark Study on Patient Privacy & Data Security,” meanwhile, reports that the average economic impact of a data breach on the organizations it looked at was $2 million.

Indeed, for healthcare organizations, the financial implications of a privacy breach go far beyond the significant fines they may pay if a breach takes place. "With devices being connected the way they are and with the malware threats increasing exponentially,” clinical and biomedical engineers must possess a basic understanding of both secure network architecture and “the threat landscape.”

— Axel Wirth, Symantec Corp.

"Security cannot be solved by IT alone, and it cannot be solved by biomed alone.”

"Indeed, for healthcare organizations, the financial implications of a privacy breach go far beyond the significant fines they may pay if a breach takes place. "With devices being connected the way they are and with the malware threats increasing exponentially,” clinical and biomedical engineers must possess a basic understanding of both secure network architecture and “the threat landscape.”

A Painful Lesson

If your department leases equipment that stores PHI, be sure you return it to the vendor, consider what happened to health insurance provider Affinity Health Plan, Inc.

In August 2013, Affinity reached a settlement with the U.S. Department of Health and Human Services (HHS), agreeing to pay $1,215,780 for potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) that occurred in 2010 when the company discovered it had failed to erase the confidential medical information of up to 344,589 individuals from the hard drives of multiple photocopiers it had leased and then returned to leasing agents. Affinity learned of the breach from CBS Evening News, which discovered the private data when it purchased one of those previously leased copiers.

In accordance with the HITECH Act’s Breach Notification Rule, which applies to HIPAA-covered entities, Affinity filed a breach report with the HHS Office for Civil Rights (OCR). Ultimately, according to OCR director Leon Rodriguez, Affinity’s penalty reflected not only the breach, but its failure to “undertake a careful risk analysis to understand the threats and vulnerabilities to individuals’ data, and have appropriate safeguards in place to protect this information.”
With that list in hand, Wirth continues, it’s time for the “technical nitty-gritty of ‘OK, what do I need to do?’ And that may be a better anti-malware strategy, or a better defensive strategy against hacking attacks. It may be staff education, or it may be encryption or implementing something like data loss prevention.” The technical execution of any security program, with its serious financial implications, has to be supported by leadership, stresses Wirth. “It cannot be operational—a couple of IT guys chasing malware and hacker attacks on computers and devices. Because really, if you think about it, the impact is not that you may lose a device or a desktop computer to a piece of malware,” it’s really about the heart and soul of your institution. “It’s about your bottom line, with the fines and lawsuits, but it also affects your reputation, operational productivity and it affects your staff. People will walk, patients will choose other hospitals if yours is on the front page of the local paper. So really, the whole topic of security, privacy, and compliance has to be driven as a business objective.”

Don’t start at the bottom and try to sell one technical fix after the next to management, says Wirth. “It really has to be coming from the top down.”

Jeff Kabachinski, director of technical development with biomedical and diagnostic imaging services provider ARAMARK Healthcare Technologies, agrees. “Working together with IT to understand where security is lacking,” he says, “and then establishing a security policy that is backed by the entire facility” so that it’s easy to enforce, will go a long way toward protecting your devices from prying eyes. And in his opinion, Kabachinski adds, “probably the No. 1 thing you can do” once that policy is developed, is “to make sure that anybody who touches a contact point in your network” knows the security basics. “Things like access rights, and don’t give away your password—all those things that we’ve heard a million times.” Remember, he says, “the clinical staff may not be tech savvy. They may not even think about it or have any idea how important those things are.” Education, therefore, is crucial. “If you can keep awareness high—if security is always on your mind—you’re much more likely to notice when something funny starts to happen.”

Mitigating Risk

At Cedars-Sinai Medical Center in Los Angeles, that round-the-clock job of mitigating risk falls to Spencer SooHoo, PhD, the facility’s chief security officer. But also, in no small way, it falls to everyone else on the Cedars-Sinai staff, including the director of clinical engineering and device integration, Jennifer Jackson, CCE. “Most of the policies and procedures that we follow in regards to PHI are the ones that Spencer and his team have laid out for us,” says Jackson. “It’s a very thoughtful and well-planned program, with everything already in place. It’s really easy to follow.”

Some highlights: First, says SooHoo, they’ve mandated encryption of all disk drives on both laptops and desktops, as well as for all messages sent over the Internet. “If you’ve got it encrypted and it goes missing, I don’t have to worry about proving that there’s no PHI out there because it’s not a breach,” he explains. “So everything’s encrypted—end of discussion.” Devices that hold PHI but don’t allow encryption, such as workstations affixed to anesthesia machines that display information from a patient’s electronic medical record, are “anchored down,” says SooHoo, “so if someone wanted to walk off with one, they’d have to walk out with the entire machine.” And then there’s the facility’s policy regarding third-party contractors: Any company hired to service equipment containing PHI must first sign a HIPAA Business Associate Agreement. That agreement, a product of last year’s HIPAA Omnibus Rule, “makes that business associate equally liable” for any breach of PHI, explains SooHoo. “It basically puts them on notice that they’d better watch what they’re doing.”

Which leads to what SooHoo and Jackson

---

**Cover Story**

**Breach News**

Interested in the latest data breach to come down the pike? Access an up-to-date list of healthcare-related breaches through the search engine provided by the consumer education and advocacy nonprofit Privacy Rights Clearinghouse at [https://www.privacyrights.org/data-breath/new](https://www.privacyrights.org/data-breath/new). The search engine includes data breaches of all sizes.

The U.S. Department of Health and Human Services also offers a breach search tool, but it only includes breaches affecting 500 or more individuals. See [www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html](http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html).

---

“If you can keep awareness high—if security is always on your mind—you’re much more likely to notice when something funny starts to happen.”

— Jeff Kabachinski, ARAMARK
call Cedar-Sinai’s most important PHI security measure: individual accountability—the idea that each time a person accesses PHI or uses a medical device that stores such information, he or she must first log on with a unique password. “EKG carts, for example, require users to identify themselves,” says Jackson. “And we’re about to integrate our infusion pumps, which will give them the ability to hold PHI, so anyone who uses those will have to log on as well.” In cases where for reasons related to business efficiency passwords or accounts must be shared—such as those involving a busy workstation in a pathology lab—“compensating controls” are established to address potential security weaknesses. That workstation, for instance, may be located in a locked room. “We basically limit the use of an account like that to a specific IP address,” says SooHoo. “And then we make sure it has limited access, so we know there are only a certain number of people who can get in there to use the system.” Sometimes, explains SooHoo, “that’s as close as we can come.”

And finally, the issue of hacking prevention and virus and malware defense. Cedars-Sinai requires all vendors to follow current best practices, notes Jackson, and puts any new vendor “through a rigorous technical assessment before we deploy their technology.” As part of that assessment, she says, “we review the need to control PHI, and if a medical device will have PHI on it,” the hospital asks that vendor all the pertinent questions, from how that information is stored, to whether they require user education. “There have been businesses with technologies where we’ve flat out said, ‘No, we’re not going to move forward with this,’ because we didn’t feel they had the basic security protection principles that we would expect.” According to SooHoo, problems sometimes arise when vendors tell them they can’t install antivirus (AV) software on their machines—mostly imaging devices or other high-speed data capture systems—“because it will void the FDA certification.” In his opinion, these vendors are avoiding having “to do the hard work of making sure that AV software will run on their system.” (This is a common ENCRYPTION TIPS

When Cedars-Sinai Medical Center made the decision to encrypt all disk drives, it was up to Spencer SooHoo, PhD, the facility’s chief security officer, to put the policy into practice. Now, he says, before any new Windows-operated device is purchased “we intercept the order to make sure the machine has a TPM”—trusted platform module—“that supports encryption.” He prefers the Enterprise version of Windows 7, which has BitLocker Drive Encryption built in (see http://windows.microsoft.com/en-us/windows7/products/features/bitlocker). “The trick is you have to have an Enterprise-class machine which has the hardware to support the encryption,” says SooHoo. “Otherwise you have to put your encryption key on a USB key, which works—if you don’t lose the key.” For Mac products, his department takes the same “give it to us first” approach, says SooHoo, noting that Apple “finally has firewalls available with encryption as well.”

As for those USB keys, since receiving a request to provide a safe way of copying data from an ultrasound machine where the user did not have the ability to load the client-software normally required for encrypted USB keys, SooHoo says he has preferred versions with built-in keypads (example: https://www.apricorn.com). “The nice thing about that is now I don’t care if it’s a Windows machine or Linux machine or whatever; until I put a pin into the keypad it’s not going to recognize the USB device.” Similarly, he says, if a USB key is stolen, “you only get 10 guesses on the pin before it auto-wipes. And even if you do guess the pin, the data that is on it is encrypted.” Your PHI, in other words, is safe.

Fuzzing

Jonathan Knudsen, principal security engineer at the IT security company Codenomicon, is an expert on fuzzing, an attack-simulation technique used to root out unknown software vulnerabilities in systems and devices. “It’s basically testing for robustness and security,” he explains. “By fuzzing, we can intentionally malform inputs into the software to see if it will cause some kind of failure.” The “good guys,” continues Knudsen, fuzz to find vulnerabilities they can fix before they provide an entry for attack. The “bad guys” fuzz to find weaknesses they can exploit.

Codenomicon sells its fuzzing tools and services to a wide variety of entities with concerns about cybersecurity, says Knudsen, and healthcare facilities are among them. And yes, he says, the typical hospital, with its interconnected computer systems, its electronic health records, and its networked medical devices, does have weaknesses. Lots of them. Put almost any hospital network through the paces—or, as Knudsen puts it, “go in there and kind of kick the tires”—“you’ll probably find vulnerabilities in everything you touch.”
complaint among security professionals, and many are pressing manufacturers to change their ways.) Nevertheless, says SooHoo, he is typically able to find a solution. “Many times, we can agree to exclude certain files from an AV scan, but in some cases where they are adamant that we not install AV software, we have an option of configuring an isolated network so that the device can only talk to the server it’s uploading data to.” He calls this approach “a last resort” because of the additional work it entails for the network team as it tracks IP addresses associated with the configuration. “But at least we lessen the chances that the vendor’s system will get infected. And if they do get nailed by a virus, it will at least be isolated.”

SooHoo notes that he and his staff “are pretty well plugged in to a lot of the security-intelligence media,” and they even subscribe to one service that monitors known hacker sites and delivers monthly briefings on the latest hacking threats. “That’s more on a global information-security level,” he says. “On a more practical level,” he holds a facility-wide meeting once a month, typically via teleconference, “where we go through the various security threats and the patches that have been released, and depending on each patch’s level of criticality, we’ll say, ‘OK, we have x number of days to apply it.’”

From the point of view of HIPAA, SooHoo explains, he and his colleagues are “taking reasonable measures” to protect PHI, whether it’s through encryption, keeping up with operating system patches, or locking down or limiting access to devices. And from a regulatory standpoint, that is what ultimately matters.

The Challenge of Legacy Devices

Documentation, agrees Richard Swim, CLES, MCSE, clinical technology team leader at Baylor Scott & White Health, is critical, especially with the implementation of the HITECH Act and its breach notification rule. If your records prove you have taken reasonable measures to ensure your facility’s PHI is secure, the chance you’ll be held liable when a device goes missing or a hacker jumps your defenses is greatly reduced.

Before Baylor Healthcare System merged with Scott & White Healthcare last September, Swim says, he helped lead Baylor’s efforts to assess its entire inventory for medical devices that stored PHI.

“We assessed over 60,000 assets total with thousands containing some element of PHI, so we decided instead to identify all those devices that were portable, that had multiple PHI items and records, and that could be easily either lost or stolen.” Searching their medical equipment database, Swim and his colleagues eventually narrowed their list of high-risk assets to just 700 devices. “That was something we could get our arms around,” he recalls.

The next step, Swim says, was to contact the manufacturers. “So we went and talked to them to see if we could encrypt those devices, and we learned for the most part that we could not because a lot of them were designed years ago when security was not a high priority. They were meant to live on their own little network, in their own little world, and everything was fine.” In the early years of HIPAA, Swim explains, the main concern was information display—ensuring, for example, that nurse station monitors were placed in such a way that the general public couldn’t see a patient’s records. It was only recently, as the need arose to have those medical devices connect to each other, that their security-related weaknesses became clear. “They just aren’t up to today’s standards.” To compensate, he says, his team has worked with manufacturers to set passwords and install antivirus programs on every device that they can. But their main tactic, by far, has been the simplest: “We literally lock the devices down. It won’t stop a determined thief, but it limits the grab-and-go.”

One of the main challenges Swim has
faced in his efforts to bolster device security involves dated operating systems. Many of the facility’s patient monitoring systems, for example, run on Windows XP—which, as of April 2014, is no longer supported by Microsoft. Meanwhile, Swim explains, because of hardware and encryption issues, “most have no upgrade path to Windows 7.” He talked to one manufacturer about this at a recent conference and was told he had two options: “He said, ‘You can upgrade to our latest architecture, or you can firewall-off the entire enterprise segment where those devices reside.’” While both options “come at a sizeable cost,” Swim notes, the good news is “the majority of the patient monitoring systems are already sitting on their own segmented network.” Still, he and his colleagues have decided to remove routers that connected to some of those networks, and have “introduced gateways that can get the data out another way.” In the end, he says, the exposure these monitoring systems have to the Internet is minimal. “And that’s obviously where the greatest risk is posed.”

**Security, Privacy, and Safety**

It may help here to make a distinction between security risks as they relate to patient privacy and the risks pertaining to patient safety. “Obviously,” says Wirth, “you need good security to protect privacy. But security does more than just protect privacy; security supports your operations, and security protects patient safety.” Encrypting data is a perfect example of a measure taken purely for the sake of protecting patient privacy, says Wirth. With encryption, a device’s PHI remains protected throughout the product’s life cycle. “So if an ultrasound machine is stolen, it’s protected. If you send it out for repair, it’s protected. When you discard it at the end of its useful life, it’s protected.” Security as it relates to operations—and, by extension, patient safety—is another thing altogether, says Wirth. “If a device is not properly secured and it is attacked or affected by malware, then yes, the data on that device is at risk and can be misused for things like identity theft or medical blackmailling. What is specific to medical devices though, are the problems that can arise on the operational side. If a device is shut down, that can affect patient care.”

---

“As we start connecting more and more medical devices that are directly feeding information into electronic health records, we create more opportunities for that information to be intercepted.”

— Ken Hoyme, Adventium Labs

Along those lines, Wirth differentiates between two fundamentally different scenarios: “One would be a deliberate attack on a single device, like an insulin pump or a pacemaker. An attack like that might put patients’ lives at risk, he says, but “so far we have no evidence” that a single-device attack has ever been launched outside of security research. The other scenario, which is common, “is networked medical devices built on commercial operating systems, where those devices are infected by common malware not because somebody is deliberately attacking them, but because they look like yet another desktop or laptop computer and they happen to be poorly protected.” Many medical device operating systems are behind in patch level and lack anti-malware or other cybersecurity technology, notes Wirth. “So what you get is collateral damage—those devices are affected and shut down,” and then risks to patient safety evolve from there. Wirth points out that there have been no reports thus far of a patient being harmed because of a malware attack. But, he says, “it’s easy to imagine” what might happen in the future.

Ken Hoyme, a medical device cybersecurity expert at Adventium Labs and co-chair of AAMI’s Medical Device Security working group, agrees. “Patient privacy has had a lot of attention,” he says, mainly because of HIPAA and the financial penalties imposed on those who fail to secure their data. “And clearly, as we start connecting more and more medical devices that are directly feeding information into electronic health records, we create more opportunities for that information to be intercepted.” Still, Hoyme notes, we shouldn’t neglect the safety aspect—“the idea that an attacker could manipulate a device to cause patient harm”—in our attempts to keep up with privacy law. “Unfortunately, there tends to be a lot of ‘faith-based’ risk management, where the

---

**Security Tips**

According to Codenomicon’s Jonathan Knudsen, any biomed department can improve its security simply by following a few basic rules of thumb.

* First, when a newly purchased or leased device arrives with a default username and password, change them before putting the device to use. “If you just go and pop that on your network anyone can reach it and get into it.”

* Second, anything on your network that is not being used should be shut down. “You can minimize your attack surface if you don’t leave things running when you don’t need them,” Knudsen notes.

* Third (and, perhaps, impossible), “don’t put any [patient data] on the Internet.” Sure, Knudsen says, making password-accessible PHI available online may win kudos from patients, but “there is usually a pretty direct tradeoff between security and convenience.”

---
Manager says, ‘I don’t believe anybody would do that,’ and therefore they don’t mitigate or try to put anything in place to prevent it from happening. But what we’ve seen in the research community is that this kind of device manipulation is possible; and we know that once somebody has demonstrated that something is possible, the likelihood that a real attack will happen in the future increases significantly.” The takeaway, says Hoyme, is that “security risks are present and we need to take them seriously,” and the only way to do so effectively is through collaboration. “Not only between hospital departments” and their respective staff, he says, “but also between hospitals and medical device manufacturers. Everyone needs to be on the same page.”

‘They’ve Read the Tea Leaves’
Collaboration, of course, is already taking place. And device security experts like Kevin Fu, associate professor of electrical engineering and computer science at the University of Michigan, say there is reason to hope we may soon see the rewards. Fu says the better manufacturers are well versed on the risk associated with cybersecurity and are designing devices accordingly—with a push in that direction from the FDA’s June 2013 draft guidance document on the subject. “They’ve read the tea leaves,” says Fu, who also directs the Ann Arbor Research Center for Medical Device Security. “And at least the ones I’ve talked to are taking security seriously.”

In fact, says Wu, he’s noticed manufacturers including security-threat models in the whiteboard stage of device development. “That did not happen with most earlier products,” he notes, and is the reason most medical devices in use today possess inherent security flaws. “What we like to say in the security business is, ‘You can’t bolt security on after the fact; you have to build it in.’ So, when you talk about things like anti-virus, that’s reactionary. That’s like, ‘Well, we didn’t get the design right, what can we do now?’ So the good news is, careful early-stage design can mitigate these problems, and I think that’s happening now.”

ARAMARK Healthcare Technologies’ Kabachinski sees similar signs of progress. Still, he feels, there’s work to be done, and device makers aren’t the only ones to blame. “Historically,” says Kabachinski, “manufacturers have been a little lacking on security aspects” in the design stage. But even as that changes, healthcare facilities will still be obligated to make security a priority, and they won’t have the luxury of just trusting their devices. “You have to protect your network, to make sure your firewall is there and hackers aren’t getting through. Or if a patient uses a smartphone to access their medical records or to download a software package so they can take their own ECG, which is then transmitted to the electronic health record database—suddenly that’s another point of contact where someone might access the network.” If hospitals are serious about PHI security, says Kabachinski, they must acknowledge that “it’s everybody’s problem—the manufacturers, leadership, physicians, IT, biomed, even the patients.”

Indeed, notes Dale Nordenberg, president of Novasano Health and Science and co-founder and executive director of the Medical Device Innovation, Safety, and Security Consortium, PHI security is everyone’s problem. As a society, “we’ve accepted the accelerated digitization of healthcare,” he says. “We’ve failed, meanwhile, “to develop and adopt the security-related best practices” that must come with it. That is changing, Nordenberg says, thanks to increasing collaboration among all the stakeholders. “But we still have a long way to go.”

References


---

**RESOURCES**

- **AMI’s 80001**
  Managing Medical IT-Networks
  www.aami.org/publications/standards/80001.html

- **Archimedes: Ann Arbor Research Center for Medical Device Security**
  A “cross-disciplinary research initiative on medical device security, privacy, safety, and effectiveness”
  www.secure-medicine.org

- **Center director Kevin Fu’s blog on medical device security and safety:**
  http://blog.secure-medicine.org

- **CE-IT: A Clinical Engineering/IT Collaboration**
  http://ceitcollaboration.org

- **Health Information and Management Systems Society (HIMSS)**
  The group’s security and privacy toolkits can be found at: www.himss.org/library/healthcare-privacy-security

- **The Health Information Trust Alliance (HITRUST)**
  HITRUST’s Common Security Framework (CSF) is “the most widely-adopted security framework in the U.S. healthcare industry.”
  www.hitrustalliance.net

- **Integrating the Healthcare Enterprise**
  “An initiative by healthcare professionals and industry to improve the way computer systems in healthcare share information.” Its vision is to “enable seamless and secure access to health information whenever and wherever needed.”
  www.ihe.net

- **Ponemon Institute**
  Conducts independent research on privacy, data protection, and information security policy
  www.ponemon.org

- **SANS Institute**
  Provides information security training, certification, and research
  www.sans.org

- **U.S. Department of Health and Human Services**
  The department provides information on privacy and security practices at: www.healthit.gov/providers-professionals/ehr-privacy-security
  It offers a summary of HiPAA at: www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html
  Find “Implementation Resources” for providers and professionals at: www.healthit.gov/providers-professionals/implementation-resources

- **U.S. Food and Drug Administration’s “Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software”**
  www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077812.htm
Congratulations to the 2014 AAMI Award Winners

Celebrating Excellence and Leadership

**AAMI Foundation Awards**
- **AAMI Foundation’s Laufman-Greatbatch Award**: Matthew B. Weinger, MD
- **AAMI Foundation & ACCE’s Robert L. Morris Humanitarian Award**: Ismael Cordero
- **AAMI Foundation & Institute for Technology in Health Care’s Clinical Solution Award**: Robert D. Butterfield

**AAMI Awards**
- **AAMI & Becton Dickinson’s Patient Safety Award**: Mark E. Bruley, CCE
- **AAMI’s HTM Leader of the Year Award**: Patrick K. Lynch
- **AAMI & GE Healthcare’s BMET of the Year Award**: Chad D. Sinclair, CBET, CRES
- **AAMI’s Young Professional Award**: Shelly Crisler
- **The Spirit of AAMI Award**: Alan Lipschultz, CCE, PE, CSP

**Standards Awards**
- **Standards Developer Awards**
  - Richard Bancroft
  - Eamonn Hoxey
  - Ronald Reitan
  - Philip Schneider
- **AAMI Technical Committee Award**
  - AAMI Electromagnetic Compatibility Committee

**TMC Bright Idea Award**
Biomedical Technology Department at Brown Mackie College:
“Polishing Soft Skills for the Future HTM Professional”

**BI&T Awards**
- **Outstanding Article**
  - “Closed-Loop Infusion Pump Integration with the EMR” by Dan C. Pettus and Tim Vanderveen.
- **Outstanding Commentary**
  - “How to Become a High-Performing HTM Department” by Heidi Horn.
- **Outstanding Research Paper**
  - “An Estimate of Patient Incidents Caused by Medical Equipment Maintenance Omissions” by Binseng Wang, Torgeir Rui, and Salil Balar.

★ Congratulations to these outstanding professionals! ★