HEALTHCARE RISK MANAGEMENT™

THE TRUSTED SOURCE FOR LEGAL AND PATIENT SAFETY ADVICE FOR MORE THAN THREE DECADES

INSIDE

NOVEMBER 2018 Vol. 40, No. 11; p. 121-132

Hacked Medical Devices Can Threaten Patient Safety

Security concerns with healthcare technology often involve safeguarding protected health information (PHI), but there is a real threat to patient safety from hackers accessing the medical devices used in treating patients. Hospitals and health systems must be proactive in addressing the risks and not rely only on device manufacturers to keep patients safe, security experts say.

The risk to medical devices grows as more and more become part of the internet of things (IoT), in which physical devices are embedded with technology to make them wirelessly accessible.

Researchers have reported exploitable vulnerabilities in Medtronic pacemakers that hackers could use to interfere with the electronic impulses that regulate patients' heartbeats. At the Black Hat cybersecurity conference in Las Vegas, security experts Billy Rios and Jonathan Butts reported on vulnerabilities they found in the Medtronic CareLink 2090 programmers. There are about 33,000 of the programs in use in the United States.

> "MANY DEVICES ARE UPDATED WIRELESSLY THROUGH THE INTERNET, AND THAT OPENS THE POSSIBILITY OF A HACKER GETTING ACCESS IN THAT WAY."

Medical device company Abbott also announced a voluntary recall of 465,000 pacemakers in 2017 due to a possible hacking threat. The FDA said the devices contained vulnerabilities that could allow access to a patient's device using commercially available equipment. This access could be used to modify programming commands to the implanted pacemaker, which could result in patient harm from rapid battery depletion or

Financial Disclosure: Author **Greg Freeman**, Editor **Jill Drachenberg**, Editor **Jesse Saffron**, Editorial Group Manager **Terrey L. Hatcher** and Nurse Planner **Kay Ball** report no consultant, stockholder, speaker's bureau, research, or other financial relationships with companies having ties to this field of study. Consulting Editor **Arnold Mackles**, MD, MBA, LHRM, discloses that he is an author and advisory board member for The Sullivan Group and that he is owner, stockholder, presenter, author, and consultant for Innovative Healthcare Compliance Group.

HEALTHCARE RISK MANAGEMENT™

Healthcare Risk Management™, ISSN 1081-6534, including Legal Review & Commentary,™ is published monthly by Relias Learning, 111 Corning Road, Suite 250, Cary, NC 27518-9238. Periodicals postage paid at Cary, NC, and additional mailing offices. POSTMASTER: Send address changes to Healthcare Risk Management, Relias Learning, 111 Corning Road, Suite 250, Cary, NC 27518-9238.
GST Registration Number: R128870672

SUBSCRIBER INFORMATION: Customer Service: (800) 688-2421. ReliasMediaSupport@reliasmedia.com ReliasMedia.com

SUBSCRIPTION PRICES: USA, Print: 1 year (12 issues) with free CE nursing contact hours, $519. Add $19.99 for shipping & handling. Online only, single user: 1 year with free CE nursing contact hours, $469. Outside USA, add $30 per year, total prepaid in USA funds.

MULTIPLE COPIES: Discounts are available for group subscriptions, multiple copies, site licenses, or electronic distribution. For pricing information, please contact our Group Account Managers at groups@reliasmedia.com or (866) 213-0844. Missing issues will be fulfilled by customer service free of charge when contacted within one month of the missing issue date. Back issues, when available, are $87 each.

ACCREDITATION: Relias LLC is accredited as a provider of continuing nursing education by the American Nurses Credentialing Center's Commission on Accreditation. Contact hours [1.5] will be awarded to participants who meet the criteria for successful completion. California Board of Registered Nursing, Provider CEP#13791.

Relias LLC is accredited by the Accreditation Council for Continuing Medical Education (ACCME) to provide continuing medical education for physicians.

Relias LLC designates this enduring material for a maximum of 1.5 *AMA PRA Category 1 Credits™*. Physicians should claim only credit commensurate with the extent of their participation in an activity.

Healthcare Risk Management™ is intended for risk managers, healthcare administrators, healthcare legal counsel, and physicians.

This activity is valid 36 months from the date of publication.

Opinions expressed are not necessarily those of this publication. Mention of products or services does not constitute endorsement. Clinical, legal, tax, and other comments are offered for general guidance only; professional counsel should be sought for specific situations.

AUTHOR: Greg Freeman
EDITOR: Jill Drachenberg
EDITOR: Jesse Saffron
EDITORIAL GROUP MANAGER: Terrey L. Hatcher
SENIOR ACCREDITATIONS OFFICER: Lee Landenberger

EDITORIAL QUESTIONS
Call Editor **Jill Drachenberg**, (404) 262-5508

administration of inappropriate pacing.

McAfee, a cybersecurity company based in Santa Clara, CA, found the potential to falsify a patient's medical vital signs in under five seconds. The company's threat research team noted that healthcare systems take advantage of and use central monitoring stations to make decisions on patient treatment and other critical care.

"This information is gathered from many IoT devices on the network using uncommon networking protocols," the team wrote in a recent blog post. "What if these devices indicate a patient was peacefully resting, when in fact they are under cardiac arrest?"

The McAfee team reported a weakness in one of the networking protocols used by medical IoT devices (the RWHAT protocol) to monitor a patient's condition and vitals. This protocol is used in some of the most critical systems in hospitals.

"The weakness discovered allows medical data to be modified by an attacker in real time to provide false information to medical personnel," McAfee reported. "Lack of authentication also allows rogue devices to be placed onto the network and mimic patient monitors." *(The McAfee blog post is available online at: https://bit.ly/2P0sacS.)*

Those incidents and reports show that the risk from medical devices is not just theoretical, says **Alan Brill**, senior managing director with the Cyber Risk Practice for Kroll in Secaucus, NJ.

"In cybersecurity, there is sometimes the tendency to hype a potential threat before anything has really happened and before it is anything more than a theory. This is not the case here," Brill says. "Rather than being a science fiction-type hype, this is a real thing that has been acknowledged by the FDA. And it's not just implantable devices that are at risk, because many devices are updated wirelessly through the internet, and that opens the possibility of a hacker getting access in that way."

The growing use of home healthcare and outpatient services is driving the use of more wireless devices that can update and transfer data over the internet, notes **Stacy Scott**, managing director with the Cyber Risk Practice for Kroll in Dallas. That creates a threat to the integrity of that data, she says.

"You can be making decisions based on data that is real-time but incorrect," she says. "Availability of data is always a big issue, but the validity of that data can be just as important or more so. Losing financial data is bad, but the scariest thing is the possibility of caregivers making decisions based on vital signs, allergy indications, or other information that is not correct."

EXECUTIVE SUMMARY

Hackers can access medical devices in ways that could jeopardize patient safety. Patients can be harmed intentionally or through the corruption of vital data.

- The threat has been proven and is not just theoretical.
- Medical devices have been recalled because of hacking vulnerabilities.
- Device manufacturers have not always built security into their products.

Scott cautions that vendors are not always the best resource for information on keeping their products safe from intrusions.

"There are badly behaved vendors who will say things like they'll lose their FDA clearance if they change anything on the device, even the password. That is simply not true," Scott says. "The bigger vendors are working toward better security and developing better processes, but you have to work with the vendors and have a good communication process. When you have a better understanding of the risks and solutions, you can communicate more effectively with the vendors."

Healthcare manufacturers have seen instances of attempted tampering with medical devices, says **James DeGraw**, JD, partner with the Ropes & Gray law firm in San Francisco.

"We've actively advised clients on situations where they suspected people were attempting to do things with their devices that they were not designed for," DeGraw says. "In one instance, the client was worried about these issues with a product that went to a large market, and there were people who had gotten hold of one and were playing with it to see what they could alter. The client had thought about this ahead of time and had designed a defense for each access point, and that worked to keep people from doing harm with the devices."

The threat to medical devices is gaining more attention from the FDA, explains **Kirk J. Nahra**, JD, partner with the law firm of Wiley Rein in Washington, DC.

"They are viewing cybersecurity as something that can potentially impact patient health," he says. "There is a regulatory interest in trying to develop standards that weren't there previously because it took years for us all to realize that this is a serious issue that can affect the health and safety of patients."

The FDA has emphasized that cybersecurity for medical devices is a responsibility shared among healthcare providers, device manufacturers, and consumers. The FDA's Center for Devices and Radiological Health (CDRH), the department responsible for regulating networked medical devices, conducts cybersecurity reviews on these devices.

"THEY ARE VIEWING CYBERSECURITY AS SOMETHING THAT CAN POTENTIALLY IMPACT PATIENT HEALTH. THERE IS A REGULATORY INTEREST IN TRYING TO DEVELOP STANDARDS THAT WEREN'T THERE PREVIOUSLY."

Recently, the FDA recognized cybersecurity standards for standard, network-connectable devices.

Major improvements probably will be driven by manufacturers who are worried about litigation or reputational harm from their devices being breached in a way that harms patients, Nahra says.

"The FDA is likely to push device manufacturers to be smart about these things from the beginning," he says. "There are lots of regulations and standards that push companies to do what they should be doing in their own self-interest anyway, and I suspect this is going to go in that direction also. The hospital also has some interest in ensuring that the vendor is taking the necessary steps to ensure the safety of the device, just as it has an obligation to verify that vendors have adequate data safety measures applying to protected health information."

Security Not Included

There is no doubt that hackers can access medical devices and cause physical harm in addition to identity theft, says **Roy Wyman**, JD, partner with the law firm of Nelson Mullins Riley & Scarborough in Nashville, TN. There are plenty of stories of individuals hacking into more complex devices, such as cars, and changing how they function, he notes.

"The basic reason is that many connected devices do not have security baked in. Particularly with older devices, manufacturers would take older, disconnected device models and simply slap on the technology to connect them to a network," Wyman says. "Security, to the extent it was addressed at all, was after the fact. Thankfully, some manufacturers are now making sure, at least with newer devices, that there is security by design in how they are developed."

That change has been largely driven by concerns about liability and heavy pushes by larger hospitals and other providers, Wyman says.

The risks vary from hacking into a device to gain access to other systems such as electronic health records (EHRs) to changing the function of the device itself. The associated risks could be loss of a significant amount

of personal health information or physical harm to patients, among others, Wyman says.

"The more savvy hospitals are reviewing the security features of these devices as well as requiring, contractually, that the manufacturers implement very specific security features to protect against such attacks," he says.

Operating Systems Vulnerable

A recent study by Virta Laboratories into post-market medical device security monitoring determined that medical devices often are shipped with older, unsupported operating systems, notes **Avani Desai,** president of Schellman & Company, a security and privacy compliance assessor in Tampa, FL.

"In fact, several medical devices in 2012 were shipped with the outdated Microsoft Windows XP operating system. As medical devices can stay in clinical use for decades, outdated operating systems may lead to a lack of patch management," she says. "This causes the device to be highly vulnerable to malware infection. As the healthcare industry is one of the top targets for malware and theft of medical records, this is a concern that needs to be mitigated early in the manufacturing process."

Tracking and location are a concern, she notes. A number of medical devices enable the tracking and geolocation of the user, a legitimate feature that has been shown to increase improvement in patient outcomes.

Desai cites the example of asthma inhalers and elder care. Several inhalers use mobile apps via Wi-Fi to collect data about location and medical information, such as the time and date of an asthma attack. In the case of elder care, general location awareness is collected from a wearable device, she explains.

The use of Wi-Fi as a means to collect and share location data can increase privacy and security concerns if not correctly implemented. This can lead to man-in-the-middle (MitM) attacks, resulting in stolen PHI and even physical security concerns, she says.

> "MEDICAL DEVICES WERE NOT DESIGNED TO BE CONNECTED TO THE INTERNET, AND WHEN THAT FUNCTIONALITY WAS ADDED, LITTLE TO NO THOUGHT WAS GIVEN TO SECURITY."

Implantable Devices at Risk

Implantable devices also are a concern. Medical devices that are physically implanted into the body (IMDs) are the most intrusive devices known, Desai notes.

Due to the devices' intimate use, IMDs pose the greatest security concerns for patients and may have potentially fatal consequences. A study on IMDs by the University of Madrid in Spain found that IMDs were subject to MitM attacks across unsecured Wi-Fi connections, she explains. The study stated that IMDs contain significant PHI such as name, address, and Social Security number — all of which are at risk of theft from eavesdropping.

"In an environment where PHI is a highly attractive commodity for a criminal, any weakness in security measures will be found. The medical device market itself is financially healthy; however, we need to remember the patient. Taking basic security and privacy measures, such as ensuring that patching of operating systems and software is achievable and performed, will help prevent breaches," Desai says.

"Nonetheless, as medical devices became ever more likely to be internet-enabled and to share data across cloud platforms, we also need to take precautions against the interception of patient data. Ensuring safe Wi-Fi implementation and setup and using encryption for data both in transfer and at rest will help to ensure a healthy outlook for medical devices and the patients who use them."

Traditionally, the IoT has focused little on privacy by design and security by design, the concept that privacy and security should be implemented at the design stage of any new product offering, says **Michael Hellbusch**, JD, an attorney with Rutan & Tucker in Costa Mesa, CA. As a result, the functional components of IoT devices often lack the proper security, leaving them vulnerable to hacking and malware attacks.

"Simply put, medical devices were not designed to be connected to the internet, and when that functionality was added, little to no thought was given to security. Now it is recognized that connected medical devices are alarmingly vulnerable to hackers who are able to gain access to and control the devices to use them maliciously," he says.

One notable example, Hellbusch notes, occurred in 2013 when doctors disabled the wireless capability of former Vice President Dick Cheney's implanted defibrillator and heart pump due to fears of potential assassination attempts via device hacking.

"Yet such concerns are not relegated to heads of state. Networked medical devices of all types bear familiar risks, including unauthorized control and access, denial-of-service attacks, and ransomware or malware," he says. "In addition, as an endpoint for hospital networks, they are another access point to an organization's data centers."

Risk assessments should include the level of security on a device, the ability to correct any gap in security, the risk of harm associated with a networked medical device (such as determining whether it is a Class I, II, or III device), and the cost of that potential harm, he says.

'Wireless' Means 'Hackable'

Any device that has wireless connectivity can be hacked — everything from mobile point of sale terminals to vacuum cleaners, says **Rami Muleys**, head of application security business development at Positive Technologies in Boston, a provider of enterprise security solutions.

"Lately, we could see increasing numbers of medical devices such as pacemakers, drug pumps like insulin infusion devices, implantable defibrillators, and other devices implementing wireless connectivity for doctors to control and fine-tune their work and update firmware. This makes these devices incredibly dangerous for patients," he says. "Potentially, a criminal could research and reverse communication protocols and exploit vulnerabilities in the simple software used in those tiny devices. For example, they could change the heart rate controlled by pacemakers or inject wrong doses of drugs or even make them show the wrong data, leading doctors to the wrong conclusions and causing them to make mistakes in their treatment."

In the report by security researchers at the Black Hat conference showing that Medtronic's CareLink 2090 programmers could be compromised, Muleys notes that they were running on Windows XP, a vulnerable and obsolete operating system no longer supported by Microsoft.

"The main reason for those risks is that the vendors are relying on the security by obscurity concept and not implementing security features on the design stage of the devices," he says.

In a security bulletin updated in October, Medtronic acknowledged vulnerabilities in its CareLink 2090 and CareLink Encore 29901 programmers and the software deployment network (SDN) for updating device software. According to the bulletin, posted on the Medtronic website, the company has taken steps to deal with the risk. "To remediate these vulnerabilities and enhance cybersecurity of device programmers, Medtronic has disabled access to the SDN." Medtronic representatives will update the software manually when needed, the bulletin states.

Muleys points out that healthcare applications became the most highly attacked of all sectors in third-quarter 2017, registering 1,526 incidents per day on average, according to findings in the Q3 2017 web application attack report from Positive Technologies.

Attacks on healthcare applications and devices had varying motivations. Throughout 2017, there were attacks aimed at gaining control of a server or accessing data. On multiple occasions, media reports described leaks of data from medical centers followed by a ransom demand sent to clinic management and patients, he notes.

Healthcare organizations concerned about security should address those risks starting with comprehensive assessments of their organization's infrastructure by security experts and white hat hackers, Muleys says. A security assessment will allow hospitals to take an inventory of the digital perimeter and internal infrastructure, identify security risks and vulnerabilities, triage them, and build a threat model appropriate for the organization, he says.

Many times, healthcare providers experience a false sense of security because of their trust in public clouds and medical software and equipment vendors, Muleys says.

"The only way to make vendors invest more in security is if the hospitals and healthcare organizations make information security a priority and ask vendors what they've done to secure their products," he says. "In the coming years, cybersecurity in treatment will be as important for patients' health as the chemical safety of drugs, but the regulation and control are on absolutely different levels."

Brill advises risk managers to conduct risk assessments that include factors such as how many devices are subject to this risk, how they are updated, how many updates have not been applied, how passwords are changed, and whether any devices have been left with the default password.

"Then you will have a much more complete picture of your risks and

your existing responses to those risks," he says. "That will yield a picture much more revealing than most hospitals have right now." ■

SOURCES

- **Alan Brill**, Senior Managing Director, Cyber Risk, Kroll, Secaucus, NJ. Phone: (201) 319-8026. Email: abrill@kroll.com.
- **James DeGraw**, JD, Partner, Ropes & Gray, San Francisco. Phone: (415) 315-6343. Email: james.degraw@ropesgray.com.
- **Avani Desai**, President, Schellman & Company, Tampa, FL. Phone: (866) 254-0000.
- **Michael Hellbusch**, JD, Rutan & Tucker, Costa Mesa, CA. Email: mhellbusch@rutan.com.
- **Rami Muleys**, Head of Application Security Business Development, Positive Technologies, Boston. Phone: (857) 208-7273.
- **Kirk J. Nahra**, JD, Partner, Wiley Rein, Washington, DC. Phone: (202) 719-7335. Email: knahra@wileyrein.com.
- **Stacy Scott**, Managing Director of Cyber Risk, Kroll, Dallas. Phone: (972) 795-3075. Email: stacy.scott@kroll.com.
- **Roy Wyman**, Partner, Nelson Mullins, Nashville, TN. Phone: (615) 664-5362. Email: roy.wyman@nelsonmullins.com.

Cybersecurity Experts Warn Hospitals About Device Security Risks

Medical devices may not be the first priority when healthcare organizations address cybersecurity, but risk managers should make sure they are included in defensive efforts, say cybersecurity experts.

Because of the pressures they face competing for cybersecurity talent and capability investment, hospitals are forced to prioritize only the most critical security functions, leaving them vulnerable to cyberattack when the threat environment changes quickly, says **Michael Figueroa**, executive director of Advanced Cyber Security Center in Bedford, MA.

Protecting medical devices is difficult because devices rarely are updated due to patient safety concerns and tend to have long-expected lifespans, he explains. Taking a more collaborative approach to cyberdefense would give hospitals more timely awareness of the threats to those devices and help them to incorporate shared intelligence from peers and the broader community to augment limited information from device manufacturers, he says.

In New England, several hospital security directors have established an informal email group list to share their threats and effective practices, Figueroa notes. Engaging with local chapters of security-oriented professional organizations and threat-sharing cooperatives would provide more support, he says.

When more formal legal frameworks are needed to prevent non-disclosure of sensitive security information, hospitals also can join community-level consortia such as the Advanced Cyber Security Center (ACSC) to build private local peer relationships and sector-specific threat-sharing organizations, such as the National Health Information Sharing and Analysis Center, to gain broader situational awareness, he suggests.

End-to-end authentication is the solution to much of the device risk, says **Mike Nelson**, vice president of IoT security at DigiCert, a company in Lehi, UT, that addresses the validity of all digital connections from secure system login for nurses and doctors to communications between devices, the network, and external databases such as electronic health records (EHRs).

"These connections are two parts in a single system. On the front end, you must verify the identity of any person using a device or accessing patient data, such as doctors and nurses," he says. "On the back end, it's just as crucial to authenticate connections between devices and the servers, EHRs, drug libraries, and other resources with which they interact."

One solution in use involves a public key certificate, also known as a digital certificate or identity certificate. This is an electronic document used to authenticate users, systems, and devices without the need for tokens, password policies, or other cumbersome user-initiated factors. This decentralizes authentication and allows it to happen across disparate systems, Nelson explains.

Security providers can offer single sign-on, multifactor authentication and patient identification to establish trust between users, technology, and the data transmitted throughout the healthcare ecosystem, he notes.

On the back end, some certificate authorities have built infrastructure capable of deploying billions of certificates to connected devices. In addition to providing identity assurance for devices connecting to servers, systems, and databases,

these authorities offer solutions for ensuring the integrity of code and the reliability of software updates, Nelson says.

"End-to-end authentication won't come to fruition in the healthcare industry until device manufacturers, hospitals, insurance companies, software vendors, and security providers recognize their shared responsibility and begin working collaboratively," Nelson says. "Some leading manufacturers are looking to address the problem before things get too painful or regulation occurs."

Nelson offers these recommendations to improve medical device security:

• **Never run unsigned code.** All software running on a medical device should be signed to ensure authenticity.

• **Never trust unauthenticated connections.** Any service that connects to a medical device should be properly authenticated.

• **Encrypt sensitive data.** Any patient data generated by the device and transmitted to another location needs to be encrypted to ensure the data are handled in a confidential way.

There is another risk associated with hackers accessing medical devices, says **Jonathan Langer**, CEO of Medigate, a cybersecurity company based in Tel Aviv, Israel. That risk involves the damage an IoT device breach can do to a hospital's or health system's network.

This danger often comes from advanced persistent threat (APT) groups, sophisticated hackers often working for a specific entity like a political group.

"Recent cyberattacks prove that APTs are actively targeting the healthcare sector. We expect to continue seeing such attacks, and therefore it would come as no surprise to see these actors targeting medical devices in order to reach sensitive information or even disrupt patient care," Langer says. "The healthcare sector should plan and revamp its dedicated cyberdefenses in order to mitigate these emerging threats."

Anything connected to your network is a potential attack vector for sophisticated hackers, warns **Troy Kent**, threat researcher with Awake Security in Sunnyvale, CA.

"All that a person with malicious intent needs is one unsecured entry point to then move laterally and access medical devices and systems holding PHI. By the same token, any IoT or connected device, such as personal devices, that's brought onto the network could become a gateway for hacking medical devices, potentially leading to physical harm to a patient," he says.

NIST Report Shows Threats to Medical Devices

A draft report from the National Institute of Standards and Technology (NIST), part of the U.S. Department of Commerce, examines cybersecurity vulnerabilities and privacy risks related to the medical devices on the internet of things (IoT).

"Many organizations are not necessarily aware they are using a large number of IoT devices. It is important that organizations understand their use of IoT because many IoT devices affect cybersecurity and privacy risks differently than conventional IT devices do," according to the draft report, titled "Considerations for Managing IoT Cybersecurity and Privacy Risks." *(More information on the report is available online at: https://bit.ly/2CMk8l9.)*

Many organizations are not aware they are using such a large number of IoT devices, the report says.

"It is important that organizations understand their use of IoT because many IoT devices affect cybersecurity and privacy risks differently than IT devices do," the draft report says. "Once organizations are aware of their existing IoT usage and possible future usage, they need to understand how the characteristics of IoT affect managing cybersecurity and privacy risks, especially in terms of risk response."

NIST recommends three risk mitigation goals:

• Protect device security to prevent a device from being used to conduct attacks, eavesdrop on network traffic, or compromise other devices on the same network segment.

• Protect data security by securing the confidentiality, integrity, and/or availability of data collected by, stored on, processed by, or transmitted to or from the IoT device.

• Ensure individuals' privacy impacted by processing of personally identifiable information beyond risks managed through device and data security protection.

Each of the risk mitigation goals requires addressing a set of risk mitigation areas, the NIST report says. ■

"At the most basic level, security practices like multifactor authentication and network segmentation are necessary. But also enabling hospital security teams to identify and respond to threats quickly," he says "The challenge here is that these teams are often blind to nontraditional attacker targets like the medical devices."

It is not always simple to spot malicious intent.

"For instance, how do you differentiate between malicious tinkering with an insulin pump vs. a legitimate change ordered by a medical professional? It all looks the same to the untrained eye, and putting the broader context together takes time and skill," Kent says. "The good news is a new breed of network traffic analysis tools can identify and profile these devices and then automate the behavioral analytics and threat-hunting needed to spot attacks."

The Manufacturer Disclosure Statement for Medical Device Security (MDS2) can be valuable in this effort to protect devices, but only if manufacturers fill it out in great detail, says **Stephanie Domas**, vice president of research and development at MedSec, a healthcare cyber security research company in Miami.

The MDS2 form focuses on security capabilities of connected medical devices. It provides medical device manufacturers with a means for disclosing to healthcare providers the security-related features of the medical devices they manufacture.

The form consists of a series of 84 yes/no questions about 19 security capabilities for the device, with a possibility to add notes at the end of each.

"The form becomes near useless to hospitals if a medical device manufacturer simply fills out the form by answering the yes/no questions, and not populating the notes fields," Domas says.

For example, with the question "Can the device display private data?" a simple yes/no answer is not particularly useful, she says. The way the form is designed, the need for a related note if the answer is "yes" is not obvious, and even manufacturers with good intentions often treat it as a yes/no exercise with no additional information.

However, when a manufacturer answers "yes" and then populates the notes field with something like "The device displays the patient age on the main screen, and the patient name can be viewed after entering nurse's credential," the form is starting to be useful, Domas says.

"The questions in the MDS2 form are good questions that aim to uncover key pieces of cybersecurity functionality a connected medical device may have. But manufacturers who simply provide yes/no answers aren't providing the hospital with the information they truly need," Domas says.

"Question 17-1 asks, 'Can the device encrypt data at rest?' Many MDS2 forms have been filled out with a simple yes or no, and no associated notes to clarify. While knowing that a device can encrypt data, it's critical for a hospital to know details such as 'Does it decrypt data by default? What type of encryption does it use? Is the key unique per system?'" ■

SOURCES

- **Stephanie Domas**, Vice President of Research and Development, MedSec, Miami. Phone: (305) 396-6900.
- **Michael Figueroa**, Executive Director, Advanced Cyber Security Center, Bedford, MA. Phone: (781) 271-5173.
- **Troy Kent**, Threat Researcher, Awake Security, Sunnyvale, CA. Phone: (833) 292-5348.
- **Jonathan Langer**, CEO, Medigate, Tel Aviv, Israel.
- **Mike Nelson**, Vice President of IoT Security, DigiCert, Lehi, UT. Phone: (801) 701-9600.

More Robust Informed Consent Needed for Telemedicine

The growing use of telemedicine is putting more pressure on risk managers to develop appropriate processes for informed consent. This modality requires an emphasis on making sure patients understand the limitations of telemedicine at the same time it is being promoted as the new, modern way to interact with healthcare professionals.

Telemedicine applications and evolving technologies are changing the consent process, says **Fay A. Rozovsky**, JD, MPH, president of The Rozovsky Group in Williamsburg, VA. The changes include what information should be discussed with the patient and how the consent for a telemedicine encounter should be documented, she says.

There are a variety of applications for telemedicine, Rozovsky notes. Care providers may use telemedicine

to interpret diagnostic imaging, pathology samples, electrocardiology, and fetal monitoring tracings. The findings may be sent to the ordering care provider in an electronic report, she notes. In urgent situations, the findings may be the subject of a real-time phone or secure email discussion.

Telemedicine also may involve a distant care provider interacting directly with a patient, either with telemetry or telepsychiatry, telepsychology, internal medicine, or specialist interactions. In those instances in which the discussion involves imaging or tracing results shared via telemedicine, the specialist can refer to and share the content with the patient during the discussion, she notes.

Another telemedicine technology enables remote care providers to see real-time diagnostic information and speak to onsite healthcare professionals and patients. One example of such technology is e-ICU.

Consent forms for "legacy processes" involving consent are unlikely to be sufficient to document a successful telemedicine consent communication, Rozovsky says.

"Although some may see telemedicine as an item that can be added to a general admission consent form, such an approach may be a setup for failure. It is prudent to consider utilizing specific consent communications and documentation for telemedicine and telehealth services," Rozovsky says.

"It should be recognized that some states have specific requirements for telemedicine and telehealth consent. It is important, too, to examine recent legislative changes in which states have added specific consent requirements for certain types of telemedicine and telehealth services such as treatment of substance abuse disorders."

State legislative changes notwithstanding, legacy processes may not be consistent with national guidelines or standards that have evolved for telemedicine and telehealth services, Rozovsky says.

Examples include the American Telemedicine Association's "Practice Guidelines for Live, On-Demand Primary and Urgent Care" and the Federation of State Medical Boards' "Model Policy for the Appropriate Use of Telemedicine Technologies in the Practice of Medicine." Rozovsky says it also is important to consider accreditation standards.

Telemedicine and telehealth are technologies that may engender some liability risks, Rozovsky says. In addition to the failure to follow applicable state laws on telemedicine or telehealth consent, she notes these risks:

- violation of scope of practice and/or licensure laws regarding which care providers can participate in such services;
- substandard practice leading to patient injury;
- delays resulting in patient injury;
- negligent treatment;
- negligent credentialing of care providers involved in telemedicine or telehealth services (note that there is a federal regulation on use of remote provider credentialing);
- breach of information security;
- breach of patient privacy;
- identity theft;
- billing and coding;
- breach of contract;
- providing unauthorized telemedicine or telehealth services;
- lack of liability, technical errors and omissions, cyberinsurance coverage.

Healthcare is increasing the pace at which it is adopting telemedicine and telehealth services, so healthcare risk managers should develop appropriate consent policies and processes for them, Rozovsky says. Working with legal counsel, risk management professionals can identify state-specific requirements, she says, and national guidelines and standards also can be incorporated into updated processes.

Aside from well-recognized core elements of consent, Rozovsky says telemedicine and telehealth discussions and documentation should address these items:

- an explanation of the process;
- who will be involved in the process;
- the limitation of telemedicine or telehealth;
- the option to seek in-person services;
- access to records by the patient and other care providers;
- any costs to the patient associated with requests to share images or reports with other care providers;
- measures taken to prevent the risk of hacking telehealth and telemedicine information;
- costs of telemedicine and telehealth services not covered under the individual's health insurance plan, especially for out of network providers, imaging, or telepathology;
- the potential for delays in interpretation or communication of results and care provider-patient discussion due to technical problems;
- specific authorizations for other uses of telemedicine and telehealth images or information in education, research, or publications.

"It cannot be emphasized enough that since many states have or are enacting laws on telemedicine and telehealth, it is important to tailor consent communication and documentation to conform to such requirements," Rozovsky says. "Additionally, in developing

telemedicine and telehealth policies, there are other considerations. Regulations on credentialing remote providers and billing and coding merit review with legal counsel and financial officials."

Most states have requirements for informed consent in telehealth, and some go so far as to dictate the required language, notes **Lisa Schmitz Mazur**, JD, partner with the law firm of McDermott Will & Emery in Chicago. Some also specify that the consent must be obtained in writing, while others allow for verbal consent, she notes.

"Even in the states where there is no specific telehealth requirement for informed consent, I still advise healthcare providers to develop a process of informed consent specific to that type of care," Mazur says.

"It gives the healthcare provider an opportunity to educate the patient on telehealth, which is good because even though it has been around a long time, it is still new to many individual patients. You can explain what the technology is, what is appropriate for, and what is not appropriate for, so that you're all on the same page from the beginning."

State issues regarding consent are especially important in telemedicine, says **Jacob Harper**, JD, an attorney with the Morgan Lewis law firm in Washington, DC. State approaches to telemedicine vary widely, he says, and it is important to comply not only with the state in which your organization resides but possibly with another state's laws as well, he says.

"Some states emphasize educating the patient about how this is not an in-person consultation and there are sometimes things that can get lost in translation," Harper says. "There is a difference in telehealth — no matter how valuable it is in the greater scheme of healthcare — and seeing a physician face-to-face. States can be particular about how they want you to explain that in the consent process."

The technology itself can present liability challenges, Harper says.

"I've seen situations where a patient tried to upload photos to show the doctor something about his condition, the pictures didn't upload for some reason, and the physician chose to proceed with the treatment without that information," Harper says. "That can create potential risk, and risk managers need to avoid those situations where care can be compromised. It's one thing where everything is working great and there are no hiccups, but everyone knows that technology can fail at the worst times."

Even when an organization determines that there is a need for specific telehealth consent, that consent process can be included in the intake along with other types of consent, Mazur notes. It it not necessary to wait until a telehealth session is scheduled to go ahead and educate the patient about that process, she says, although it may also be prudent to go over the material again for future telehealth appointments.

Mazur notes that some of the same concerns with video telehealth can apply when data is transmitted from the patient's home but without any audiovisual interaction. This may apply for telemetry of patient vitals and other data. There also can be unique concerns with telemetry.

"It's very important when you're talking about remote patient monitoring to provide the patient with information about when the doctor is going to review the data," Mazur says. "You want the patient to understand that the doctor is going to review this data, but they may not be reviewing it in real time on a consistent and constant basis. If a cardiac monitor records a cardiac arrhythmia, the doctor may not see that until the next patient visit. You don't want the patient thinking that is constantly monitored in real time."

The goals for telemedicine consent should be similar to any other type of consent, hinging on good communication and documentation, says **Richard Cahill**, JD, vice president and associate general counsel with The Doctors Company, a liability insurer in Napa, CA. However, that does not mean that a standard, traditional consent process for treatment is sufficient for telemedicine, he says.

He notes that the Federation of State Medical Boards (FSMB) has developed a model policy for telemedicine consent, addressing such concerns as establishing a doctor-patient relationship remotely.

"State licensure is a key concern and physicians should be educated on this, as it applies even if the patient is out of state on vacation," he says.

The FSMB's "Model Policy For The Appropriate Use of Telemedicine Technologies in the Practice of Medicine" outlines six specific consent issues that should be addressed.

(The model policy is available online at: https://bit.ly/2RSkTNW.)

As with all consent processes, informed consent for telehealth must be carried out by the physician and cannot be delegated, Cahill says.

"Patients need to be advised of the material facts, based upon their actual circumstances, based on community standards, in a way and using terminology that the patient can reasonably understand," Cahill says. "The standards for informed

consent are not diminished in any way because the care is being provided in a telehealth setting, though there are additional challenges that also must be addressed."

Consent issues arise whenever there is a new way to deliver healthcare, notes **Samuel J. Louis**, JD, an attorney with the Clark Hill law firm in Houston. Telehealth presents challenges for risk managers not because it is new, but because it is now becoming more widely used than ever before, Louis says.

"Whenever there is some new aspect of delivery systems for healthcare, it is important to make sure the patient has a clear understanding of what services are being provided, what the risks are, and that therefore their consent is knowing and voluntary," Louis says.

The limitations of telemedicine are particularly important in the consent process, Louis says. Patients must understand that the physician is unable to conduct assessments they might see in a traditional face-to-face office visit.

"In a traditional encounter, the physician relies not only on what the patient is saying but there also is the opportunity to examine the patient and conduct various hands-on assessments, whereas in telemedicine you don't have that option," Louis explains. "The physician is limited in the ability to determine the root cause of the patient's problem, but the patient may have a true physical encounter with a physician later who makes a different assessment, or the lack of that physical assessment may lead to the patient suffering some type of harm. The patient who accepts a telemedicine encounter must understand those limitations so that the liability is limited for the provider." ■

SOURCES

- **Richard Cahill**, JD, Vice President and Associate General Counsel, The Doctors Company, Napa, CA. Phone: (800) 421-2368.
- **Jacob Harper**, JD, Morgan Lewis, Washington, DC. Phone: (202) 739-5260. Email: jacob.harper@morganlewis.com.
- **Samuel J. Louis**, JD, Clark Hill, Houston. Phone: (713) 951-5604. Email: sam.louis@clarkhillstrasburger.com.
- **Lisa Schmitz Mazur**, JD, Partner, McDermott Will & Emery, Chicago. Phone: (312) 984-3275.
- **Fay A. Rozovsky**, JD, MPH, President, The Rozovsky Group, Williamsburg, VA. Phone: (860) 242-1302.

CME/CE QUESTIONS

1. **Which of the following is true regarding cybersecurity of medical devices?**
   a. Abbott announced a voluntary recall of 465,000 pacemakers in 2017 due to a possible hacking threat.
   b. There has not yet been any mandatory or voluntary recall of a medical device due to a possible hacking threat.
   c. The FDA has recommended the recall of Abbott pacemakers because of security concerns, but the manufacturer refused to recall the products.
   d. Abbott intended to recall pacemakers over a possible hacking threat, but the FDA refused to allow the recall.

2. **According to Stacy Scott, which of the following is true regarding alteration of a medical device's settings?**
   a. Any alteration of the device settings, including the password, will result in the manufacturer losing FDA clearance for the product.
   b. Device settings, including the password, may be altered to improve security without the manufacturer losing FDA clearance for the product.
   c. A healthcare provider should rely on the factory settings to ensure the best security for a medical device and not alter them.
   d. Changing device settings usually has no effect on the security of a medical device.

3. **What is one important issue to emphasize in the consent process for telemedicine?**
   a. The limitations of telemedicine
   b. The specific type of equipment used in the encounter
   c. The amount of money saved by using telemedicine instead of an office visit
   d. The provider's criteria for selecting physicians allowed to use telemedicine

4. **What does Lisa Schmitz Mazur, JD, recommend regarding the use of telemetry?**
   a. Advise the patient about when the data will be reviewed by a physician.
   b. Prohibit the use of telemetry from the patient's home except in the most extreme need.
   c. Require that telemetry data be reviewed by a physician in real time.
   d. Do not make any statement about how the data will be reviewed.

HEALTHCARE RISK MANAGEMENT™

DocuSign Envelope ID: E7020DC4-AE47-4AE5-B602-96D3F9FEC6AF

Statement of Ownership, Management, and Circulation
UNITED STATES POSTAL SERVICE® **(All Periodicals Publications Except Requester Publications)**

1. Publication Title	2. Publication Number	3. Filing Date
Healthcare Risk Management	1081-6534	10/1/2018
4. Issue Frequency	**5. Number of Issues Published Annually**	**6. Annual Subscription Price**
Monthly	12	$519.00

7. Complete Mailing Address of Known Office of Publication *(Not printer) (Street, city, county, state, and ZIP+4®)*
111 Corning Rd, Ste 250, Cary, NC 27518

Contact Person: Joshua Scalzetti
Telephone *(Include area code)*: 919-439-1751

8. Complete Mailing Address of Headquarters or General Business Office of Publisher *(Not printer)*
111 Corning Rd, Ste 250, Cary, NC 27518

9. Full Names and Complete Mailing Addresses of Publisher, Editor, and Managing Editor *(Do not leave blank)*

Publisher *(Name and complete mailing address)*
Relias LLC, 111 Corning Rd, Ste 250, Cary, NC 27518

Editor *(Name and complete mailing address)*
Jill Drachenberg — 111 Corning Rd, Ste 250, Cary, NC 27518

Managing Editor *(Name and complete mailing address)*
Jesse Saffron — 111 Corning Rd, Ste 250, Cary, NC 27518

10. Owner *(Do not leave blank. If the publication is owned by a corporation, give the name and address of the corporation immediately followed by the names and addresses of all stockholders owning or holding 1 percent or more of the total amount of stock. If not owned by a corporation, give the names and addresses of the individual owners. If owned by a partnership or other unincorporated firm, give its name and address as well as those of each individual owner. If the publication is published by a nonprofit organization, give its name and address.)*

Full Name	Complete Mailing Address
Relias LLC	111 Corning Rd, Ste 250, Cary, NC 27518
Bertelsmann Learning LLC	1745 Broadway, New York, NY 10019

11. Known Bondholders, Mortgagees, and Other Security Holders Owning or Holding 1 Percent or More of Total Amount of Bonds, Mortgages, or Other Securities. If none, check box → ☒ None

Full Name	Complete Mailing Address

12. Tax Status *(For completion by nonprofit organizations authorized to mail at nonprofit rates) (Check one)*
The purpose, function, and nonprofit status of this organization and the exempt status for federal income tax purposes:
☒ Has Not Changed During Preceding 12 Months
☐ Has Changed During Preceding 12 Months *(Publisher must submit explanation of change with this statement)*

PS Form **3526,** July 2014 *(Page 1 of 4 (see instructions page 4))* PSN: 7530-01-000-9931 **PRIVACY NOTICE:** See our privacy policy on *www.usps.com.*

DocuSign Envelope ID: E7020DC4-AE47-4AE5-B602-96D3F9FEC6AF

13. Publication Title: Healthcare Risk Management
14. Issue Date for Circulation Data Below: September 2018

15. Extent and Nature of Circulation			Average No. Copies Each Issue During Preceding 12 Months	No. Copies of Single Issue Published Nearest to Filing Date
a. Total Number of Copies *(Net press run)*			214	199
b. Paid Circulation *(By Mail and Outside the Mail)*	(1)	Mailed Outside-County Paid Subscriptions Stated on PS Form 3541 (Include paid distribution above nominal rate, advertiser's proof copies, and exchange copies)	164	150
	(2)	Mailed In-County Paid Subscriptions Stated on PS Form 3541 *(Include paid distribution above nominal rate, advertiser's proof copies, and exchange copies)*	0	0
	(3)	Paid Distribution Outside the Mails Including Sales Through Dealers and Carriers, Street Vendors, Counter Sales, and Other Paid Distribution Outside USPS®	1	1
	(4)	Paid Distribution by Other Classes of Mail Through the USPS (e.g., First-Class Mail®)	19	16
c. Total Paid Distribution *[Sum of 15b (1), (2), (3), and (4)]* ▶			184	167
d. Free or Nominal Rate Distribution *(By Mail and Outside the Mail)*	(1)	Free or Nominal Rate Outside-County Copies included on PS Form 3541	11	11
	(2)	Free or Nominal Rate In-County Copies Included on PS Form 3541	0	0
	(3)	Free or Nominal Rate Copies Mailed at Other Classes Through the USPS (e.g., First-Class Mail)	0	0
	(4)	Free or Nominal Rate Distribution Outside the Mail *(Carriers or other means)*	3	3
e. Total Free or Nominal Rate Distribution *(Sum of 15d (1), (2), (3) and (4))*			14	14
f. Total Distribution *(Sum of 15c and 15e)* ▶			197	181
g. Copies not Distributed *(See Instructions to Publishers #4 (page #3))* ▶			17	18
h. Total *(Sum of 15f and g)*			214	199
i. Percent Paid *(15c divided by 15f times 100)* ▶			93%	92%

* If you are claiming electronic copies, go to line 16 on page 3. If you are not claiming electronic copies, skip to line 17 on page 3.

DocuSign Envelope ID: E7020DC4-AE47-4AE5-B602-96D3F9FEC6AF

Statement of Ownership, Management, and Circulation
UNITED STATES POSTAL SERVICE® **(All Periodicals Publications Except Requester Publications)**

16. Electronic Copy Circulation	Average No. Copies Each Issue During Preceding 12 Months	No. Copies of Single Issue Published Nearest to Filing Date
a. Paid Electronic Copies ▶		
b. Total Paid Print Copies (Line 15c) + Paid Electronic Copies (Line 16a) ▶		
c. Total Print Distribution (Line 15f) + Paid Electronic Copies (Line 16a) ▶		
d. Percent Paid (Both Print & Electronic Copies) (16b divided by 16c × 100) ▶		

☐ **I certify that 50% of all my distributed copies (electronic and print) are paid above a nominal price.**

17. Publication of Statement of Ownership
☒ If the publication is a general publication, publication of this statement is required. Will be printed in the November 2018 issue of this publication. ☐ Publication not required.

18. Signature and Title of Editor, Publisher, Business Manager, or Owner
Bjorn Bauer — Bjoern Bauer — Bjoern Bauer — Chief Financial Officer — Chief Financial Officer
Date: 19-Sep-2018

I certify that all information furnished on this form is true and complete. I understand that anyone who furnishes false or misleading information on this form or who omits material or information requested on the form may be subject to criminal sanctions (including fines and imprisonment) and/or civil sanctions (including civil penalties).

LEGAL REVIEW & COMMENTARY
EXPERT ANALYSIS OF RECENT LAWSUITS AND THEIR IMPACT ON HEALTHCARE RISK MANAGEMENT

Hospital Liable for $29.5 Million for Delayed Treatment of Allergic Reaction During CT Scan

*By **Damian D. Capozzola**, Esq.*
The Law Offices of Damian D. Capozzola
Los Angeles, CA

***Jamie Terrence**, RN*
President and Founder, Healthcare Risk Services
Former Director of Risk Management Services (2004-2013)
California Hospital Medical Center
Los Angeles, CA

Nathan Jamieson
UCLA School of Law
JD Expected May 2020

News: A female patient visited a hospital complaining of mild constipation. The treating physician ordered a CT scan for the patient. The hospital administered an intravenous dye to enhance the CT results.

The patient suffered an allergic reaction to the dye and almost immediately lost consciousness. The physician administered only Benadryl during the first 45 minutes. After 45 minutes, the physician treated the patient with epinephrine; however, the patient had already suffered severe brain damage. The patient ultimately succumbed to the brain damage later that evening.

The patient's estate and her children brought suit against the physician and hospital, claiming that the delay in treating the patient with epinephrine was negligent and caused the death. The patient's attorney asserted that absent the delay in treatment of epinephrine, the patient would have survived. A jury returned a $29.5 million verdict in favor of the plaintiffs.

Background: The patient, a 40-year-old mother of four, presented to a local clinic, complaining of mild constipation. The treating physician ordered a routine CT scan. The patient was administered intravenous contrast dye to better highlight blood vessels, organs, and other internal structures.

Minutes after the dye was administered, the patient suffered an anaphylactic reaction, losing consciousness and going into shock. She was treated only with Benadryl during the first 45 minutes of the reaction, and the physician failed to take the patient's vital signs as well. The patient suffered severe hypoxic brain damage.

AFTER 45 MINUTES, THE PHYSICIAN TREATED THE PATIENT WITH EPINEPHRINE; HOWEVER, THE PATIENT HAD ALREADY SUFFERED SEVERE BRAIN DAMAGE.

Approximately 45 minutes later, the physician treated the patient with epinephrine after her heart stopped beating; however, she had suffered severe, irreversible brain damage from which she later died. Her husband and four children thereafter brought suit against the hospital and physician, alleging malpractice.

During trial, the plaintiffs' expert contended that the physician's failure to timely administer epinephrine fell below the applicable standard of care owed to patients and that had the physician administered this drug earlier, the patient would not have suffered the brain damage. The plaintiffs' expert also contended that the physician's failure to assess the patient's vital signs constituted malpractice. The hospital and physician categorically denied these contentions, claiming that timely administering epinephrine would not have prevented the injury and subsequent death.

The jury found in favor of the plaintiffs, with a verdict of $29.5 million to her husband for loss of consortium and to her children for the loss of their mother. An appeal from the hospital and physician is pending.

What this means to you: This serious injury and significant verdict demonstrate the requirement not only that hos-

pitals must create effective policies and procedures for patients experiencing adverse outcomes but actually implement and follow those procedures. The jury, in finding for the plaintiff, affirmed that minor mistakes can create major damages and malpractice liability. Here, the plaintiffs' expert convinced the jury that Benadryl is not an adequate response when a patient loses consciousness because of an allergic reaction. Further, the expert convinced the jury that physicians must proactively take and monitor vital signs, particularly when the patient is in distress. In short, the jury recognized that it is neither acceptable nor routine for a patient to slip into unconsciousness following a CT scan and that something must have been missed in the first instance of diagnostic testing.

While the injection of contrast dye during diagnostic radiological procedures is common, allergic reactions to the contrast medium also are common. Before proceeding, it is incumbent on the physician to ask the patient if he or she has any allergies, especially to foods like shellfish or drugs that contain iodine. If the patient is allergic, he or she is at high risk of allergic reaction to the dye. Even if the patient claims to not have allergies, physicians and staff should anticipate and be prepared for allergic reactions; drugs and equipment required for an immediate response must be readily available. Someone, most likely the treating physician, should be trained in advanced cardiac life support (ACLS) and must be prepared to implement the appropriate care in case of an unexpected reaction. If such a significant allergic reaction occurs and the patient loses consciousness, mechanical and/or chemical resuscitation should begin immediately.

Hospitals should ensure that staff are trained to maintain the patient's ventilation and circulation until the medications given to reduce the patient's allergic response take effect. It also is critical that the patient never be left alone during the administration of the contrast. Staff must frequently and regularly ask the patient how he or she is feeling. Any unusual symptoms may require that contrast administration stops and rescue efforts start immediately. Epinephrine is typically the first drug used.

Assessing for an increase in respiratory rate and pulse, cold clammy skin, chest pressure, or pain is essential once an allergic response is noticed. A crash cart filled with emergency drugs and supplies is essential. A defibrillator for addressing a possible cardiac arrhythmia or arrest is essential as long as staff are trained to use it. While many radiology departments do not have all of these items in every room, they should be close enough to access quickly with a notification system in place to send equipment and trained staff to the patient right away.

This case also shows that physicians should avoid thinking that a normally safe medication is incapable of causing severe side effects, particularly when something is overlooked or missed. The jury recognized that merely because a chemical rarely causes side effects does not mean the chemical cannot cause side effects. Although contrast dye rarely produces this degree of harm, once an allergic reaction is noted, the physician should immediately begin treatment, anticipating and/or expecting that the reaction may get worse before it gets better. Physicians owe a duty of care to patients to ensure the remedial efforts provided both address the reaction and do no further harm. In this case, Benadryl was insufficient and the physician and hospital's failure to timely realize this fell below the standard of care.

Another insight from this case is for insurers. The plaintiff here contended that the parties were unable to settle because the insurer's counsel believed that no jury in the rural area where the case was being tried would award a significant sum, a position that proved incorrect. Also, according to the plaintiffs' attorney, the insurance company thought rural juries would not feel comfortable awarding a verdict of this degree and consequently refused to settle, telling the jury that, even if the jury were to find for the plaintiff, the plaintiff was only entitled to several hundred thousand dollars. Based upon the sizeable verdict, the jury rejected this suggestion.

This verdict shows hospitals, physicians, insurers, and counsel that the involvement of a rural jury does not always equate to judgments worth pennies on the dollar and, as a corollary, that multimillion-dollar judgments are not the exclusive domain of a jury composed of city-dwellers. Egregious facts remain egregious facts even when considered by a rural jury, and here the jury clearly thought that no mother should die from a routine CT scan. Hospitals and physicians may consider retaining independent counsel even when an insurer bears the primary coverage and provides counsel. An independent counsel may ensure that the insurance-appointed counsel continually acts in the insured's best interest and avoids expensive mistakes such as rejecting settlement talks because of an erroneous assumption that a jury will not feel comfortable awarding a significant sum based on incorrect assumptions. ■

REFERENCE

Decided on June 14, 2018, in the District Court for Sioux County, Iowa; 33 Nat. J.V.R.A. 8:3.

Psychiatrist Liable for Excessive Prescribing, Leading to Patient's Death and $2 Million Verdict

News: A psychiatrist prescribed her patient multiple psychoactive medications to deal with his anxiety and other psychological issues. Despite the medications, the patient's conditions continued to worsen.

The physician increased the dosages of multiple medications without, as the patient's family later alleged, adequate monitoring of the patient. At one point, the psychiatrist prescribed the patient 80 mg per day of Celexa. The FDA, however, had previously issued a warning informing physicians that Celexa should not be prescribed at a dose higher than 40 mg per day due to the risk of cardiac abnormalities. Nonetheless, the physician did not adhere to the FDA warning and did not monitor the patient. The patient died on Nov. 12, 2013, as a result of cardiomyopathy. The coroner concluded that the patient had toxic levels of Celexa and another drug that the psychiatrist had prescribed.

On May 16, 2018, a jury returned a $2 million verdict in favor of the plaintiff. The jury concluded that the clinic was 53% liable and the psychiatrist was 47% liable. The jury awarded the decedent $1 million for emotional distress and suffering while he was still alive and his parents $1 million for loss of companionship.

Background: The patient was a 46-year-old male who suffered from anxiety and other psychological disorders. In 2009, a psychiatrist took the patient under her care and prescribed a litany of medications to treat schizoaffective disorder and severe anxiety. These medications included Clozaril, Celexa, Xanax, Haldol, and Cogentin. The physician steadily increased the dosage of his medication in the years that followed despite no indication that the medications were working to ease his psychological issues.

In 2011, the FDA issued a warning about Celexa, stating that at high doses Celexa may cause cardiac abnormalities. The FDA warning also affirmed that a high dosage of Celexa did not increase its efficacy. Consequently, the FDA warned physicians that they should not prescribe Celexa at a dose higher than 40 mg per day. This warning specifically informed physicians that they should consider more frequent ECGs for patients who are taking concomitant medications, as in this case.

Nevertheless, the psychiatrist failed to heed the FDA warning. In 2012 and 2013, the physician prescribed Celexa at a dosage of 80 mg per day in addition to the patient's other medications. According to the lawsuit, the patient dutifully took all of his medications but kept reporting that his psychological issues were worsening.

The patient died on Nov. 12, 2013, from toxic levels of Celexa and Cloziral. His parents brought suit against the clinic and the physician, contending that the physician negligently prescribed Celexa in excess of 40 mg per day in contravention to the FDA warning advising against such high doses, that the physician failed to advise the patient or his parents of the FDA's warnings, and that the physician failed to monitor his cardiac health. Specifically, the parents alleged that the physician should have recommended that the patient undergo cardiac evaluations including an ECG examination. The plaintiff alleged that these failures constituted actions below the standard of care.

The physician categorically denied the allegations and contended that the patient's obesity, poor eating habits, and sedentary lifestyle were the actual and proximate causes of his cardiomyopathy and death.

The jury found in favor of the plaintiff, finding the physician 47% liable and the clinic 53% liable. The jury concluded the plaintiffs suffered a loss of companionship and emotional distress, awarding them $1,000,000, and concluded that the patient endured pain and suffering, awarding the decedent $1,000,000. The parents used the award to establish a foundation that is committed to ensuring that hospitals and physicians understand, follow, and communicate drug warnings.

What this means to you: Medical care providers, including physicians, clinics, and hospitals, are responsible for keeping up-to-date about any newly discovered side effects or dangers inherent in the drugs they prescribe to their patients. Ongoing treatment using medication is not simply a matter of prescribe and forget. Rather, the privilege to prescribe drugs brings with it a duty to stay informed about any warnings and to proactively monitor a patient's response to those drugs. A physician who continues to prescribe medication without continuing to monitor developments pertaining to those medications, especially those in FDA warnings, may fall below the standard of care as reasonable physicians in similar circumstances

would heed new developments and warnings.

Providers must be diligent in routinely checking for FDA warnings, known as black box warnings, for all medications they prescribe. Moreover, physicians should consider the consequences, including the potential for an adverse reaction and the potential for side effects, whether merely ordering an increase in dosage or prescribing a new medication. A physician should not think that ordering an increase in dosage is a less consequential action than prescribing a new medication. Rather, physicians must understand that prescribing excessive doses may cause significant damage and produce liability as it did here. Before increasing a dosage for a known and used medication, physicians should ensure that the FDA has not promulgated any updated warnings.

Further, it is not the patient's duty to monitor and keep updates on FDA warnings — it is the medical care provider's responsibility. Both the hospital and the outside pharmacy where the patient purchased his prescriptions have a duty to patients, in addition to the physician prescribing medications. Pharmacists are required to review medication profiles on inpatients in hospitals and clients who purchase medication from retail pharmacies.

Pharmacists are the keepers of the FDA black box warnings and are duty-bound to question unusual dosing, drug interactions, and the impact of black box warnings on patients and clients receiving medications from their pharmacy. Pharmacists are required to question physicians about medication orders that pose a threat to the well-being of patients and can refuse to fill controversial doses or dangerous combinations of drugs. Most often, a simple phone call to the prescribing physician resolves the issue. If, however, the physician fails to respond to warnings, the pharmacists can proceed to fill the prescription but can be held liable if efforts are not made to advise physicians and warn patients.

Another important lesson from this case is that a patient's failure to improve may not justify an increase in the dosage of medications. To the contrary, this case reflects that a physician owes a standard of care requiring an intellectual inquiry into whether an increase in dosage will likely result in increased efficacy and, further, whether the increased efficacy is worthwhile given the harms present in an increased dosage, if any.

Physicians must be especially cautious when prescribing multiple medications to one patient or when prescribing any new medication to a patient who already takes a multitude. This is known as polypharmacy and is particularly dangerous when prescribing multiple psychoactive and psychotropic medications. Here, the physician prescribed Celexa, Clozirol, Xanax, Haldol, and Cogentin. All of these medications may trigger severe side effects, and the combination of multiple medications may exacerbate such side effects. The plaintiff's attorney asserted that physicians must be cautious of any effect these medications may cause when combined together. As such, physicians should consider seriously whether multiple medications should be prescribed and whether the potential benefit is worth the unknown risk of combining medications. Physicians should avoid the gut reaction that adding one more medication to a patient's otherwise robust medication regimen is inconsequential.

While it was the physician who prescribed the excessive medication, the clinic was assigned greater liability.

This is a valuable lesson for hospitals, clinics, and medical centers and demonstrates the need for policies and monitoring of physicians' prescribing tendencies. When new or updated FDA warnings arise, hospitals should circulate this information to physicians to protect patients and to protect the hospital from potential malpractice. Hospital ignorance is not a defense to a death caused by the excessive prescribing of medications with known side effects at high doses.

The peer review process, required in all healthcare institutions where physicians practice, includes a duty to monitor all aspects of physician performance, with a focus on positive patient outcomes, patient safety, physician competency, and frequency of adverse events that result in litigation. The hospital pharmacists can and should participate in this process by providing data from their department that can pinpoint a safety issue of concern involving a physician.

In short, medical care providers involved in any aspect of the chain of prescribing medications must be diligent in checking for newly updated warnings for any medications the physicians have currently prescribed and possibly change a patient's regimen based on these updated warnings. Physicians must exercise increased prudence when treating patients who are taking multiple medications in order to prevent such instances and to foster a patient's overall health and well-being. ■

REFERENCE

Decided on May 16, 2018, in the Court of Common Pleas of Pennsylvania, Fifth Judicial District, Allegheny County; Case Number GD-15-017525.