35th Anniversary

Healthcare RISK MANAGEMENT

AUGUST 2014 | VOL. 36, NO. 8 PAGES 73-84

Infant abductions hit all-time low, but older children still at risk

Prevention efforts successful, but watch for complacency

As of May, American hospitals had gone 21 months without an infant being abducted from one of their facilities, which is the longest time ever since data has been collected on this crime. The good news indicates that healthcare providers have gotten the message about abduction prevention, but some experts point out that teen-agers are more likely to be taken or leave on their own.

Infant abduction is high on the list of nightmares that every risk manager wants to avoid, and providers have taken several precautions in recent years, including the use of proximity alarms on infants, tighter security on obstetrical floors, increased vigilance by staff, and education for parents about the risks. Despite the lack of abductions, those precautions are warranted because there have many attempted abductions, says **John B. Rabun**, ACSW, director of infant abduction response at the National Center for Missing & Exploited Children (NCMEC) in Alexandria, VA. The attempts failed because of heightened awareness by staff and parents or because the physical security assets worked, Rabun says.

"Since we know there have been scads of potential attempt abductions, many coming in through the ED, my hat's off to all our healthcare folks for keeping the target hardened" by implementing safeguards that make the hospital a difficult place to abduct a child, he says. "My fear is our success might lend itself to complacency, if we're not careful," Rabun says.

That complacency might occur more with older pediatric patients rather than infants,

HRM recognized for outstanding analysis

Healthcare Risk Management is proud to receive a first place award in Best Interpretive or Analytical Reporting from the Specialized Information Publishers Association (SIPA). The award recognizes an article in the May 2013 issue, "CPR refusal highlights risk of overly strict policies," which addressed the lessons from an incident in which a nurse working at an assisted living home refused to perform CPR on a resident. *HRM*'s coverage of this highly publicized case went deeper than the general media's outrage. It analyzed the difficult choices that our readers can face. In addition to explaining the details of the case not previously known to most readers, *HRM* provided practical advice on how to assess current policies and avoid unintended consequences that can harm patients. ✦

INSIDE

AHC Media

www.ahcmedia.com

FINANCIAL DISCLOSURE: Author **Greg Freeman**, Executive Editor **Joy Daughtery Dickinson**, and Nurse Planner **Maureen Archambault** report no consultant, stockholder, speaker's bureau, research, or other financial relationships with companies having ties to this field of study.

he says. NCMEC recently compiled information from their database showing 1,689 children were reported missing from healthcare institutions between 2000 and 2013. Notably, 1,591 of them were "endangered runaways," who are minors who are not in the care of their parents, exposed to danger from life on the street, and prone to run away from the hospital. In most cases, the endangered runaways left of their own volition, Rabun explains. Family abductions accounted for 77, non-family abduction accounted for six, and the circumstances were unclear in 15 cases. The data suggests that while preventing infant abduction is important, risk managers might need to expand those efforts to include older children.

The runaways, whether they are teen-agers or younger, must be considered endangered, Rabun says, and their absence should be taken seriously. "If we lose a kid, even if it's because the kid ran away, there is still liability there, and we have to do our part to get law enforcement involved and find him," he says. "Hospitals have to treat children and teen-agers, and they bring the rest of their life with them. Some will be in the midst of family dissolution cases such as divorce or custody battles, and some will be unwilling to stay for different reasons. We can't turn the hospital into a juvenile detention center and lock everybody up, but we have to recognize that losing a child is serious business, even if it is not an infant."

The NCMEC data on runaways offers an opportunity to encourage more vigilance with older pediatric patients and particularly those who are troubled, says **Staca Shehan**, director of the case analysis division at the NCMEC. "It's clear from the numbers that the healthcare community has taken seriously the risk of infant abductions, and the data also shows that they could have a real impact on these older children who sometimes need someone to intervene," Shehan says. "The awareness of child safety in healthcare has increased significantly in recent years, and this data directs us to where we can have even more impact."

Executive Summary

Infant abductions from healthcare facilities are decreasing. While this signals success with prevention efforts, some worry that providers will become complacent.

- ✦ Abductions remain rare, but vigilance is warranted because of the impact.
- ✦ Older children also are at risk.
- ✦ Always notify local law enforcement before an abduction drill.

Older kids not protected as well

The philosophy on protecting children older than infants is similar to that for preventing newborn abductions, but it is complicated by the fact that older children can run away on their own. Still, hospitals can apply some of the same prevention efforts and expect similar success, he says.

As with infant abduction, the tricky part for a risk manager is to address the risk without overdoing it. The statistics on missing children and teen-agers, though higher than for infants, still don't indi-

Healthcare Risk Management® (ISSN 1081-6534), including HRM Legal Review & Commentary™, is published monthly by AHC Media, LLC, 950 East Paces Ferry NE, Suite 2850 Atlanta, GA 30326. Telephone: (404) 262-7436. Periodicals Postage Paid at Atlanta, GA 30304 and at additional mailing offices.

POSTMASTER: Send address changes to Healthcare Risk Management®, P.O. Box 550669, Atlanta, GA 30355.

AHC Media, LLC is accredited as a provider of continuing nursing education by the American Nurses Credentialing Center's Commission on Accreditation. This activity has been approved for 15 nursing contact hours using a 60-minute contact hour.

Provider approved by the California Board of Registered Nursing, Provider #14749, for 15 Contact Hours.

This activity is valid 24 months from the date of publication.

Healthcare Risk Management® is intended for risk managers, health system administrators, and health care legal counsel. 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.

Executive Editor: Joy Daughtery Dickinson (404) 262-5410 (joy.dickinson@ahcmedia.com). Director of Continuing Education and Editorial: Lee Landenberger.

SUBSCRIBER INFORMATION

Customer Service: (800) 688-2421 or fax (800) 284-3291, (customerservice@ahcmedia.com). Hours of operation: 8:30 a.m.-6 p.m. Monday-Thursday; 8:30 a.m.-4:30 p.m. Friday.

Subscription rates: U.S.A., 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 U.S., add $30 per year, total prepaid in U.S. funds. Discounts are available for group subscriptions, multiple copies, site-licenses or electronic distribution. For pricing information, call Tria Kreutzer at 404-262-5482. 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. (GST registration number R128870672.)

cate they are common at hospitals. The potential impact of losing a child is great enough, however, to warrant prevention efforts.

Many hospitals regularly conduct Code Pink drills for infant abductions, Rabun notes, but not as many devote the same effort to older children with Amber Alert drills. *(For more on Code Pink and Amber Alert drills, see the story on p. 76.)*

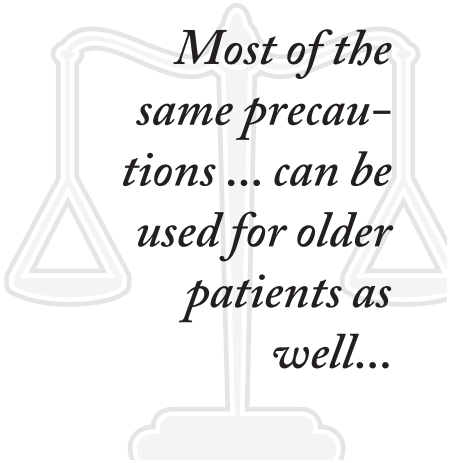
"When I travel to hospitals I see targets that are pretty well hardened, even if they may be missing a few pieces, mostly because they don't understand the profile of the offender," Rabun says. "Are hospitals more secure for infants than they were 10 years ago? Oh yes. But can you say that necessarily about [older] pediatrics? It's safer, but probably not on the same level as the newborns."

Most of the same precautions that have proven effective in neonatal units can be used for older patients as well, says **David LaRose**, MSCJ, CHPA, CPP, director of safety, security, and emergency management at Lakeland (FL) Regional Medical Center. He also is president-elect of the International Association for Healthcare Security and Safety, based in Glendale Heights, IL. Think of protecting all children at the hospital with one policy that includes staff and parent education, and then tailoring some precautions to fit the different age levels, he suggests.

Security bracelets can be used for older children as well as newborns, for example, although LaRose notes that teenage patients might refuse to wear them. *(See the story on p. 76 for more on technological solutions.)*

"A lot of hospitals declare their pediatric unit security-sensitive the same way they do with perinatal, so you have the same access control, staff intervention, and parent education," Larose says. "There is a consistent return on investment when you can utilize the same technology, the same staff and parent education, to address older children. You won't have to start from scratch looking for a solution and paying for new ways to address the risk."

In addition to Code Pink drills for infants, Lakeland Regional conducts Amber Alert drills for older children.



The drills are an opportunity to spot any deficiencies with technology or staff and parent education, as well as policies and procedures that might be improved, LaRose says. A particular concern is training new staff quickly so there are no lapses.

Encourage parents: Stay overnight

At South Nassau Communities Hospital in Oceanside, NY, infant and older pediatric security are addressed with one prevention and response plan, says Director of Nursing **Gayle Somerstein**, RN. Her hospital has addressed pediatric security for years by extending infant security precautions to older children as well.

"Whatever is done in our maternal child area is done throughout the facility for pediatric patients as well," she says. "Anyone 17 and under gets tagged with a transponder, and the pediatric unit is a locked unit accessed only by people with credentials and a reason to be there."

To improve security for older pediatric patients, especially those who might run away, Somerstein's hospital allows parents or a designated family member to visit 24 hours a day and strongly encourages them to stay with the child during the day and at night.

Rabun notes that he is not familiar with any situation in which a family sued a hospital after a child ran away or a non-custodial parent took him or her. He suspects there have been informal settlements in which the hospital quietly offered some type of compensation, either monetary or in the form free healthcare, to avoid a lawsuit.

"I think that's rational," Rabun says. "We're seeing much better capture of intake information at the pediatric level, because in many of the cases in which a parent stole a child it was because the other parent didn't say anything that would let the nurses take precautions."

Nurses or admissions clerks should ask the parent or parents admitting the child whether there is anything going on at home "that might impact your child's stay here with us." If that prompts a blank stare from the parents, Rabun says, follow up with examples: "Any family issues like a divorce or custody dispute, family disagreements, anything like that?" The query can bring forth information that the parents might not otherwise have offered because they thought the hospital staff would not be interested or be able to do anything about it. When the nurses know that parents are in a custody dispute, for example, they can be on alert and check identification.

"Abductions by family members are potentially very bad situations, even though it's the child's own mother or father," Rabun points out. "Unlike an infant abduction where the person desperately wants a child, these children are objects of spite, not objects of love. That can lead to at least a neglect situation, if not something much worse."

Sources

- David LaRose, MSCJ, CHPA, CPP, Director of Safety, Security, and Emergency Management, Lakeland Regional Medical Center, Lakeland, FL. Telephone: (863) 687-1179. Email: david.larose@lrmc.com.
- John B. Rabun, ACSW, Director, Infant Abduction Response, National Center for Missing & Exploited Children, Alexandria, VA. Telephone: (912) 786-4826. Email: jrabun@ncmec.org.
- Staca Shehan, Director, Case Analysis Division, National Center for Missing & Exploited Children, Alexandria, VA. Telephone: (912) 837-6446. Email: sshehan@ncmec.org.
- Gayle Somerstein, RN, Director of Nursing, South Nassau Communities Hospital, Oceanside, NY. Telephone: (516) 632-4974. Email: gsomerstein@snch.org. ✦

Don't rush to high-tech solutions without assessment

A needs assessment is necessary to determine the child abduction risks and potential solutions for any particular hospital, says **John B. Rabun**, ACSW, director of infant abduction response at the National Center for Missing & Exploited Children (NCMEC) in Alexandria, VA.

Too often, he says, hospitals jump to implement expensive technological solutions without really understanding their true needs.

Rabun recalls an incident at a hospital that delivers about 8,000 babies per year, with a freestanding women's pavilion. Hospital leaders asked Rabun to join their committee formed to address the infant abduction risk. He was surprised to see the committee meeting with one technology vendor after another, looking for the right tagging system.

When he pointed out that they had not conducted a needs assessment to determine if a tagging system was even necessary, hospital leaders explained that two of their much smaller sister hospitals in the same healthcare system had purchased tagging systems with funds raised by local civic organizations, and it looked bad for the big hospital not to have one.

"I could see how the C-suite folks might think that way, but I didn't see the data to support that decision," Rabun says. "Just because of the way the hospital was built, it was target-hardened. Some facilities are built so that it's not impossible, but it's pretty darned hard to get in there and walk out with a child. They had egress delay on all the fire stairwell doors, and all the elevators all opened into a common lobby that was staffed 24 hours a day by people trained to watch for people with babies and check IDs."

The hospital did a needs assessment and decided to go ahead with a tagging system, but one that was less elaborate and configured differently than what they originally had planned. ✦

Amber Alert drill a little too realistic for hospital

When one Oregon hospital conducted an Amber Alert drill for a missing child recently, hospital officials got more of a response than they intended. No one had notified the police that it was just a drill, and so four police cars went roaring to the hospital with lights and sirens.

They got word that it was a drill just before arriving, but the local police chief still was not happy about the mix-up. He issued a statement saying the emergency response put his officers and citizens at risk, and it could have been avoided with a simple phone call.

A hospital spokesman says the Amber Alert protocol requires someone to call the local emergency dispatch center to announce the drill, but apparently the person reported a child abduction to dispatchers without saying it was only a drill. Hospital officials promised to correct the problem in future drills.

Police responded to drill

A Code Pink drill at another facility, this one in Texas, prompted a police response last year, notes **John B. Rabun**, ACSW, director of infant abduction response at the National Center for Missing & Exploited Children (NCMEC) in Alexandria, VA. The hospital has a local police officer stationed at the hospital around the clock, and when the Code Pink was called over the intercom, he radioed the abduction to police dispatch. No one had notified him of the drill.

"This is exactly why we always advise the local facility to notify their neighborhood police command of a drill," Rabun says. "More often than not, the report has come from an excited new mom in a room on postpartum," who doesn't know it's a drill and calls 911 in a panic. So it's not enough to be sure no hospital employee calls 911 to report an abduction; someone else might do it for you.

Involve the police

Involving the police in the drill can be productive, Rabun notes.

He recalls once talking by phone with a charge nurse immediately after an infant was abducted. She was frustrated that the police has responded so enthusiastically that all the hospital entrances were sealed with yellow crime scene tape and she was being told to shut down all hospital operations. No one would be allowed in or out of the hospiotal until the baby was found.

Rabun asked to speak with the police commander on the scene and pointed out to him that it was about 6 p.m. and new fathers all over the city were leaving work and hearing on the news that a baby was missing from the hospital. He asked the commander if he had children, which he did, and he asked how many officers it would take to keep *him* from getting inside the hospital to check on them. "We probably don't have enough officers for that," he responded.

Rabun suggested that the police not close down the hospital entirely, but to strictly monitor those entering and leaving, and to allow the fathers to use one designated elevator to go the mother's room and see the baby. They were told they must remain in the room unless going directly to and from the elevator.

"You have to be happy to see the police respond with gusto, but they also need to know how a hospital works and that you can't just shut it down like you would a crime scene at a restaurant," Rabun says. "Working with them ahead of time can help them respond in the best way." ✦

Alternative risk financing could be right for you

Executive Summary

More healthcare providers are moving toward alternative risk financing. The strategy can result in significant cost savings and even a positive financial contribution.

- ✦ Self-insuring means starting your own insurance company, in effect.
- ✦ Consider this option if you spend more than $1 million per year in premiums.
- ✦ A captive will substantially improve the risk manager's stature.

Alternative risk financing is not just for the biggest players in healthcare anymore. Long used by large health systems, this type of self-insurance is becoming more attractive to smaller institutions as well.

Healthcare providers are all looking for ways to become more proficient in their operations, so more and more C-suite executives are looking at the option of self-insuring, says **Eileen F. Conlon**, managing director for the insurance broker Beecher Carlson in Miami.

"It behooves the risk manager to be familiar with this type of risk financing, how it works and, why you might consider it, because it is something that is going to be on the radar screens of their senior management," Conlon says.

Alternative risk financing is a mechanism that allows cost savings because you carve out some of the costs incurred when dealing with an insurance company, Conlon explains. With a typical insurance policy, the healthcare provider pays a premium to the insurer, who in turn pays on some claims. With self-insurance, the hospital sets up its own insurance company, known as a captive or a risk retention group, and sets aside the money it would have paid in premiums but avoids the administrative costs associated with a commercial insurer. Premiums paid to the captive are invested for the benefit of the healthcare provider rather than sitting in an insurance company's bank account.

"Money not paid out by the captive is retained by the healthcare provider, so if you have a particularly good year with minimal claims losses, that can contribute substantially to the bottom line," Conlon says. "Even if it is only a small sum, that adds up over time, and the interest grows. Hospitals that have had a captive in place for 30 years or even more are seeing very significant amounts of money that can be reallocated to other uses."

Forming a captive will require hiring accounting professionals, attorneys, a reinsurance broker, and a captive manager. The provider is not completely on its own when it comes to managing and paying claims, however. Most healthcare providers have re-insurance that will kick in after a claim reaches a specified threshold, such as $1 million in costs, or after all claim expenditures total $10 million for the year.

The option has been mostly used by large health systems and hospitals, but Conlon says that situation is changing as leaders realize the potential benefits. After years of paying for insurance and analyzing claims, healthcare providers might realize that they could achieve the same results while saving themselves some money.

"We're seeing it more now in smaller systems, and smaller practices like physician groups are looking to do this," Conlon says. "The typical guideline is that if you're spending more than a million dollars a year in premiums, a captive is something you should be looking at."

Another important consideration is how well you manage claims. The captive – you, essentially – handles all claims management unless the reinsurance kicks in, so you have to be confident that you can do that task. Also consider your risk management and patient safety records. Are you doing outstanding work in those areas, and do you not expect many claims? Or is there a lot of room for improvement?

Some providers are drawn to self-insuring because they think their good records in claims and loss management are not being recognized by commercial insurers, notes **Geoffrey Etherington**, JD, partner in the New York City office of Edwards Wildman, which specializes in insurance. Particularly for smaller clients, insurers might refuse to tailor coverage and premiums for good performers, he explains. The hospital is lumped in with other providers who might have much worse records, which results in a higher premium.

In addition, self-insuring might allow the healthcare provider to obtain insurance that is not available to it on the open market, Etherington says. "For example, a facility that provides long-term care for children may feel like they have some child abuse exposure and need coverage for that," he explains. "That might be hard to find, or they might not be able to find it at the coverage amounts they want."

Self-insuring usually leads to better claims management because you're doing it yourself, Conlon says. Senior managers also are more interested and responsive to risk management when they know that the hospital will be paying the claims directly rather than letting an outside insurance company take the hit. That involvement can help risk managers improve safety, she says. (*See the story on p. 78 for more on the risk manager's role with a captive.)*

Etherington cautions that any provider considering a captive should work closely with accountants from early in the consideration process and all the way through forming the captive.

"Sometimes people assume that a captive program will allow them to fully deduct the premiums they pay to the captive, but that's actually a very complicated question and has to be analyzed carefully," he says. "You don't want to get to the end of the year with your tax returns or financial statements and find that your attorneys or accountants are not willing to sign off on the structure."

Sources

• Eileen F. Conlon, Managing Director, Beecher Carlson, Miami. Telephone: (305) 704-5415. Email: econlon@beechercarlson.com.

• Geoffrey Etherington, JD, Partner, Edwards Wildman, New York City. Telephone: (212) 912-2740. Email: getherington@edwardswildman.com. ✦

Risk manager plays key role with captive

Self-insuring means taking on more responsibility for managing claims and minimizing losses, and the risk manager plays a key role, says **Eileen F. Conlon**, managing director for Beecher Carlson in Miami.

The risk manager will be intimately involved with the captive's claims management, and the importance of patient safety and managing risk will become clearer to senior management. "If the risk manager starts seeing an increase in emergency department claims, for instance, it will be obvious to everyone in management that fixing the problems there will save money for the hospital," she says. "Whereas you might have had to fight for what you knew was right for patient safety, now the tie to lost dollars will be obvious to everyone. It's a straight line from the patient safety issue to the captive writing a check, rather than the idea of letting the insurance company handle it."

Risk managers also will be instrumental in the decision-making progress when considering this option. Senior managers will look to the risk manager as the person best able to assess the claims record and areas of risk, Conlon says. The risk manager's stature within the facility will improve, especially if it goes ahead with the self-insurance plan.

"It helps garner the risk manager an audience with their senior management, which might mean obtaining additional resources to improve patient safety," Conlon says. "Self-insuring tends to create much more recognition of the importance of the risk manager's job." ✦

Electronic communications still a major risk

Despite years of regrettable incidents and cautions about social media and other forms of electronic communication, healthcare providers still are at risk from rogue or careless employees who post patient information or other inappropriate material on the web. It is proving more difficult than many originally thought to monitor social media and to prevent staff from posting in a way that makes the hospital liable.

The pervasiveness of social media is part of the problem, but so is the way online communicating has become second nature, says **Jimmy Lin**, vice president of product management and corporate development at The Network, a governance risk compliance company in Norcross, GA. Something funny happens at the office happy hour, so why not tweet about it? The hospital had an interesting case, so someone shares the news on Facebook. (See the story on p. 79 for two recent examples.)

Employees often do these things naturally and don't even think they could be putting themselves and the provider at risk for reputation damages and potential lawsuits, Lin says. A recent trend is even more worrisome, however. "We're seeing hospital employees who post pictures of patients from a particularly awful accident, and it's not just sharing with a few friends," he says. "There seems to be a real desire for these pictures in the market, and so people are supplying them. The pictures can go viral and once they're out there, you can't get them back. It can lead to liability that the poster never expected."

Risk managers must educate employees about how to communicate safely, but Lin suggests doing it in the way tech fans like their information: short bursts of information from their smartphones. Use social media to train employees about social media. "These are the heavy users that you want to reach the most, so you should do it with frequent reminders and messages sent to their phones or Facebook," he explains. "That targets the right people. Think about smaller chunks over a long period, rather than a long employee training session."

Healthcare providers also should monitor social media for any information about or stemming from the hospital, Lin suggests. The sooner you know about a confidentiality breach or other improper posting, the sooner you can work to mitigate the damage.

Policies must be clear about the use of social media, but employers have to realize that it is here to stay, says **Joanna Belbey**, social media and compliance specialist at governance provider Actiance in New York City. Healthcare employees frequently use social media legitimately to communicate with each other and patients, she notes, so the best strategy is to provide guidance on how to use it

Executive Summary

Healthcare providers still experience liability risks from employees' use of social media and other electronic communications. Sharing information online has become second nature to many.

- ✦ Tailor compliance education to the way these people communicate.
- ✦ Provide examples of what is and is not allowed when posting online.
- ✦ Monitor social media for references to your facility.

properly. "Once you develop policies on social media use, the next step is to show employees how those policies apply to their specific situations," Belbey says. "Provide a lot of examples, and let people discuss why one is acceptable and the other is not. It is important to not only show them what not to post, but what they can post online."

There are some legal limitations on how much an employer can restrict an employee's posts or discipline the employee for posting, says **Howard M. Miller**, JD, member of the law firm Bond Schoeneck and King in Garden City, NY. The law still is evolving in this area, he says, but the National Labor Relations Board (NLRB) is studying how much censorship is too much, especially with union employees. Employees can be prevented from violating laws by posting patient information, for example, but how much you can restrict comments about the employer is less clear.

"Generally you can't stop certain griping about working conditions," Miller says. "But there are legitimate concerns about putting information online that is damaging to the reputation of the employer, so it's a question of where the line is, and we haven't found it yet."

Sources

- Joanna Belbey, Social Media and Compliance Specialist, Actiance, New York City. Telephone: (650) 631-6300.
- Jimmy Lin, Vice President of Product Management and Corporate Development, The Network, Norcross, GA. Telephone: (800) 253-0453. Email: jimmyLin@tnwinc.com.
- Howard M. Miller, JD, Member, Bond Schoeneck and King, Garden City, NY. Telephone: (516) 267-6318. Email: hmiller@bsk.com. ✦

Sexting in surgery, Facebook post among latest problems

Two recent examples show how electronic communications still can be a headache for risk managers in healthcare.

In the first incident, a woman who was being treated for a sexually transmitted infection at the University of Cincinnati (UC) Medical Center is suing the hospital for more than $25,000 in damages for invasion of privacy, emotional distress, malice, and negligence. She alleges that an employee posted her medical records to Facebook, according to the lawsuit filed in Hamilton Common Pleas Court. The woman's lawsuit claims that a screen shot of her medical record showing her name and her diagnosis of syphilis was posted to Facebook in September 2013. The photo also was emailed to some Facebook users, the lawsuit claims.

In addition to suing the hospital, the woman also is suing two employees, only one of them named, of UC Medical Center and her ex-boyfriend. The lawsuit claims that the employees posted her records online at the request of the ex-boyfriend. It also alleges that UC Medical Center negligently supervised the named employee and has not done enough to identify the second.

"As a result of the inaction (of the hospital) ... the plaintiff's medical records are still in the possession of the other (unknown) employee and the plaintiff is receiving phone calls harassing her and her child," the lawsuit says.

UC Medical Center CEO **Lee Ann Liska** sent a memo to the hospital's employees in which she acknowledged the lawsuit and its claims. The memo, which was reported in several media outlets, also reminds employees that "the unauthorized access or viewing of medical records, or the unauthorized sharing of PHI [protected health information], is a serious violation of federal medical privacy laws and regulations and cause for immediate termination." It is not known if any employees were disciplined or dismissed.

MD accused of sexting in surgery

In another case, the Washington State Medical Board suspended a Seattle anesthesiologist after investigating allegations that he "sexted" during surgery, at one point sending 45 sexually explicit messages during a single operation. The board suspended Arthur Zilberstein's license for a "lack of focus" and putting patients at risk during cesarean deliveries, labor epidurals, an appendectomy, and other procedures, according to a Washington state medical board's statement of charges.

The board also investigated claims that Zilberstein sent X-rated selfies, wearing his hospital scrubs and badge with his genitals exposed.

"Oh. And my partner walked in as I was pulling up my scrubs. I'm pretty sure he caught me," Zilberstein wrote in one text message, according to the board.

Doctor tested patient

The statement of charges included claims that the doctor sent multiple sex-related messages to the same woman, a patient, and invited her to visit the hospital for sex.

He told her she could park in the doctor's lot instead of paying for parking, according to the claims, and the pair allegedly arranged to meet in the doctor's lounge or hospital call room for sexual encounters.

In addition, the statement of charges says Zilberstein obtained the unnamed woman's medical records "not for medical purposes, but in order to view images of the patient for his own sexual gratification."

The Washington state health department investigated after receiving two complaints, one from a patient and another from a healthcare professional, the report notes. Zilberstein is appealing the suspension. ✦

Electronic security a growing concern in healthcare

The Federal Bureau of Investigation's (FBI) warning on the vulnerability of healthcare data systems to cyber attack isn't the first alert to providers, but it got the attention of many who did not realize how hackers see them as a prime target.

Beginning in April, the FBI has been warning healthcare providers their cybersecurity systems are lax compared to other sectors, according to information obtained by Reuters. *(The full article is available online at http://tinyurl.com/oexvwl8.)* Hackers want in to healthcare data systems because personal medical records and health insurance data are far more valuable to hackers on the black market than credit card numbers. The health-related data usually contains details that can be used to access bank accounts or obtain prescriptions for controlled substances.

"The healthcare industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely," the FBI notice to healthcare providers says.

The threat to healthcare data is changing how some providers look at vendors they would have to trust with that data, says **Mick Coady**, principal and co-leader of the Health Information Privacy and Security Practice at PricewaterhouseCoopers, the financial services and consulting company in St. Louis, MO. The risk manager and security or compliance officer more often are invited to the meetings in which a vendor's data security is discussed and assessed, he says. This invitation represents a shift from seeing data security as primarily a tech issue to seeing it more as a risk management concern, he says.

"We're seeing that shift already in the larger institutions, and it will come to the others in time," Coady says. "As the Office of Civil Rights grows and becomes stronger, everyone is going to start looking at data security in a new light. Healthcare institutions will see more of a melding among these roles because they will realize that this is not just an IT issue, but an issue in which you have to assess the legal and liability risks on a regular basis."

Brian Lapidus, senior vice president with the fraud consulting firm Kroll in Nashville, TN, agrees that cyber security is no longer just an IT concern but is now a function of enterprise risk management. Focusing primarily on the "cyber" aspect of data security can be a mistake, he warns, because the human component is such a driver.

"It is important to look across all departments that use technology and focus on addressing exposures across the board," Lapidus says. "Go to all those departments and find out what security they're using, what is the key data they use, where is it, who has access to it, how long does it stay in the system, and who is responsible for it."

In many cases, the person you ask will have the wrong answer or no answer at all, he says. That step leads you to opportunities for better education, but it also signals a potentially weak area that could allow a hacker in. *(See the story on p. 81 for advice on improving security.)*

Technology can open your system to outside threats before you realize the technology is in use, Lapidus says. Different types of devices that create Wi-Fi hot spots and similar connections can allow a hacker access to the system or at least to passwords and other information from a user. "It can be a challenge to stay current with all the ways that someone can get into your system, but unfortunately that's what is necessary to keep your data safe," Lapidus says. "Ideally you want this approach of watching for new threats to become part of your culture so that it's not just the concern of one person, but everyone is watching for problems."

Managing flash drives with protected healthcare information (PHI) can be a challenge, notes **Joseph Wager**, MS, RCP, senior risk management and patient safety specialist for the Cooperative of American Physicians in Los Angeles. PHI stored on a USB flash drive should be encrypted with an accredited Federal Information Processing Standard (*Publication 140–2*) cryptology, he says. That is a particular type of encryption established by the National Institute of Standards and Technology in Washington, DC. *(More information is online at http://tinyurl.com/crjwbx. See* Publication FIPS 140-2.)

There is good news

The good news is that many flash drive manufactures are selling compliant devices. Most secure USB flash drives use some form of the Advanced Encryption Standard (AES) encryption, either 128-bit or 256-bit, Wager says. These levels are approved by the U.S. government for encrypting secret-level and top-secret-level documents and are compliant with the Health Insurance Portability and Accountability Act (HIPAA). A standard USB flash drive can be made compatible by adding encryption software, Wager says.

"Renting a car that has a Bluetooth system may allow the copying of all your smartphone's information: sensitive data/patient phone numbers, websites, por-

Executive Summary

Healthcare data is vulnerable to hackers in several ways. The threat is changing the role of some healthcare managers.

- The Federal Bureau of Investigation (FBI) recently warned healthcare providers of the danger.
- Health data is more valuable to hackers than credit card numbers.
- Encryption is your friend.

tals. Ask the rental agency to remove or delete your personal data when returning the car," he says. "Restaurants' and coffee shops' free Wi-Fi also opens you up to HIPAA violations. You do not have a business associate agreement with each of them!"

Sources

• Mick Coady, Principal and Co-leader, Health Information Privacy and Security Practice, PricewaterhouseCoopers, St. Louis, MO. Telephone: (314) 565-1949. Email: mick.coady@us.pwc.com.

• Brian Lapidus, Senior Vice President, Kroll, Nashville, TN. Telephone: (615) 320-9800. Email: brian.lapidus@kroll.com.

• Joseph Wager, MS, RCP, Senior Risk Management and Patient Safety Specialist, Cooperative of American Physicians, Los Angeles. Telephone: (800) 252-7706. ✦

Essential education on cyber security in healthcare

These essential steps to your facility's cyber security were provided by **Joseph Wager**, MS, RCP, senior risk management and patient safety specialist for the Cooperative of American Physicians in Los Angeles:

1. Make sure your IT department has implemented these basics and taught them to all staff:

• Make sure your system has a competent firewall installed and activated.

• Always have an efficient anti-spyware and anti-virus program.

• Do not open any attachments or files from your e-mail if you don't recognize the sender.

2. Educate all staff members on these issues:

• what constitutes a potential data security incident;

• misuse of sensitive information, such as posting of patient information on a social website;

• potential malware infections;

• dangers of losing laptop or other electronic storage devices, or hard-copy documents;

• requirement to report any of the above to the risk management and IT departments. ✦

Hospital cuts medmal 50% in obstetrics

A Connecticut hospital saw a 50% drop in malpractice liability claims and payments when it made patient safety initiatives a priority by training doctors and nurses to improve teamwork and communication, hiring a patient safety nurse, and standardizing practices, according to a study by researchers at the Yale School of Medicine in New Haven, CT.

The results, published in the June 9, 2014, online issue of the *American Journal of Obstetrics and Gynecology*, come at a time when mounting concerns about liability are thinning the ranks of obstetricians in the United States, says author **Christian Pettker**, MD, associate professor in the Department of Obstetrics, Gynecology & Reproductive Sciences at Yale School of Medicine.

"Liability insurance rates are not controlled, malpractice awards continue to increase, and there is increasing awareness of litigiousness in clinical practice," Pettker says. "As a result, obstetricians are increasingly reducing or dropping out of practice, and future physicians are discouraged from entering the field."

In 2004, Pettker and his team partnered with their liability insurance carrier to conduct a comprehensive safety assessment.

The team then made improvements to the healthcare system and culture by standardizing care, learning and practicing new teamwork protocols, and enhancing oversight of clinical work. The hospital hired a patient safety nurse, for example, and established specific ways in which clinicians would work as a team to care for an expectant mother and child.

Comparing two time periods

The team compared the five-year period before the safety program was implemented to the five-year period afterward.

"We found a 50% reduction in liability claims and also found that the payments made for these liability claims decreased 95%, from over $50 million to under $3 million," Pettker says.

In two prior studies, Pettker and his team found that the same safety-improvement program reduced adverse outcomes and created an improved culture of safety on obstetrical units. "This new publication demonstrates yet another positive result of our program," he said. "We've found that standardizing care, improving teamwork and communication, and optimizing oversight and quality review reduces liability exposure."

Pettker says that while most of the measures in the hospital's program make sense to outside observers, some involve substantial and systematic changes that might be resisted by nurses and doctors who value individual knowledge, skills, and experience.

"We don't think that this is a cure to the medical liability crisis, but this is certainly one approach that can both make things safe for the patient and have tremendous improvements and reduce a lot of the costs in healthcare that go to the defense of medicine and liability," Pettker says.

Source

Christian Pettker, MD, Associate Professor, Department of Obstetrics, Gynecology & Reproductive Sciences, Yale School of Medicine, New Haven, CT. Telephone: (203) 785-3091. Email: Christian.pettker@yale.edu. ✦

Nonpunitive response to errors top list of hospital concerns

Hospitals are struggling with finding ways to address errors without punishing those responsible, according to the Hospital Survey on Patient Safety Culture by the Agency for Healthcare Research and Quality (AHRQ) in Rockville, MD.

In response to requests from hospitals interested in comparing their results with those of other hospitals, AHRQ established the Hospital Survey on Patient Safety Culture comparative database. The first user comparative database report, released in 2007, included data from 382 U.S. hospitals. The 2014 user comparative database report displays results from 653 hospitals and 405,281 hospital staff respondents.

The report also includes a chapter on trending that presents results showing change over time for 359 hospitals that administered the survey and submitted data more than once.

The three areas of strength or composites with the highest average percent positive responses were:

• **teamwork within units** (81% positive response) — the extent to which staff support each other, treat each other with respect, and work together as a team;

• **supervisor/manager expectations and actions promoting patient safety** (76% positive response) — the extent to which supervisors/managers consider staff suggestions for improving patient safety, praise staff for following patient safety procedures, and don't overlook patient safety problems;

• **organizational learning and continuous improvement** (73% positive response) — the extent to which mistakes have led to positive changes and changes are evaluated for effectiveness.

The three areas that showed potential for improvement, or with the lowest average percent positive responses, were:

• **nonpunitive response to error** (44% positive response) — the extent to which staff feel that their mistakes and event reports are not held against them and that mistakes are not kept in their personnel file;

• **handoffs and transitions** (47% positive response) — the extent to which important patient care information is transferred across hospital units and during shift changes;

• **staffing** (55% positive response) — the extent to which there are enough staff to handle the workload and work hours are appropriate to provide the best care for patients.

The full report is available online at http://tinyurl.com/pma6pqw. ✦

Hospital to pay $41 million to settle fraud claims

King's Daughters Medical Center in Ashland, KY, will pay nearly $41 million to the federal government to settle fraud claims related to the hospital's cardiac program.

The hospital faced allegations that it billed Medicare for heart procedures performed on patients who didn't need them. King's Daughters issued a statement saying the settlement was not an admission of wrongdoing. The hospital "made the difficult decision to settle the investigation, rather than continue to drain valuable resources on government allegations related to old cases," according to the statement.

In March, more than 500 former patients of King's Daughters Medical Center sued the hospital for allegedly performing cardiac procedures they didn't need. King's Daughters issued a statement at that time saying the hospital "intends to defend the care provided by our cardiac program, of which we are very proud, and which has been recognized for its patient care and quality outcomes." ✦

Wrong kidney removed — malpractice suit follows

A man in Fort Worth, TX, is suing his urologist and radiologist after having the wrong kidney removed in surgery performed at a medical center.

Glenn Hermes, 55, underwent surgery at Plaza Medical Center in Fort Worth in 2013 to remove his left kidney because of cancer. The surgical team removed the left kidney, but soon after Hermes was told that the cancer actually was in his right kidney, according to court documents. The cancerous portion of the right kidney was removed, but now Hermes might face dialysis, a transplant, or the possibility of taking expensive drugs.

The hospital is not named in the lawsuit seeking more than $1 million in damages.

Patient noticed a growth

According to court documents, Hermes had a doctor's appointment because he was having pain near his scrotum and that he also noticed a growth near his right testicle. Hermes was told that the lump was at "high risk" of being cancerous, and doctors recommended surgery to remove the kidney, the lawsuit states.

The next month, Hermes had the surgery. Afterward he and his family were told afterward that the left kidney with a mass was removed and sent to a pathologist for analysis.

The pathology report indicated the kidney that had been removed was healthy. Another doctor recommended a partial removal of the right kidney. ✦

Sutter invests million in lifts to improve patient safety

The not-for-profit healthcare system Sutter Health recently announced an $11.5 million commitment to install overhead patient lifts at 19 intensive care units and acute rehabilitation centers across its Northern California network. Three years ago, the Sacramento-based network invested an initial $11.5 million to install overhead lifts at 21 affiliate sites.

Overhead patient lifts make repositioning and moving patients easier, safer, and less dangerous for caregivers. Initial outcomes from Sutter-affiliated hospitals with overhead lifts show that employee injuries from lifting and repositioning patients have dropped by more than 50% since 2011. The not-for-profit network anticipates even better outcomes as it installs additional lifts and employees become more familiar with using them, said **Dan Perrot**, Sutter Health's director of employee health and safety, in a sttatement about the investment.

The lifts enhance patient safety and clinical quality by allowing employees to turn and move patients in a manner that reduces risks of patients developing painful skin ulcers or experiencing falls, Perrot said. Also, the lifts allow physical therapy staff to provide early mobilization therapy to patients in intensive care units.

Perrot said, "The lifts supplement existing safety programs and equipment already in place across our network, such as mobile floor lifts, sit/stand devices, and patient mobilization programs."

The announcement brings the healthcare network's commitment to install overhead patient lifts across its network to $23 million. ✦

HRM makes move to per-issue testing

Here's a change we know you'll like: From now on, there is no more having to wait until the end of a six-month semester or calendar year to earn your continuing education credits or to receive your credit letter.

Log on to www.cmecity.com to complete a post-test and brief evaluation after each issue. Once the completed evaluation is completed, a credit letter is e-mailed to you instantly.

If you have any questions, please call us at (800) 688-2421 or outside the United States at (404) 262-5476. You also can email us at: customerservice@ahcmedia.com. ✦

Correction in July *HRM*

On page 68 of the July 2014 issue of *Healthcare Risk Management*, the Chicago-based hospital consortium UHC was incorrectly identified as part of UnitedHealthcare.

The two groups are not affiliated. ✦

COMING IN FUTURE MONTHS

✦ Best advice for preventing falls at your facility

✦ C-suite strategies for risk managers

✦ Credentials that risk managers must have

✦ Limiting C-sections at your hospital

CNE OBJECTIVES

Upon completion of this educational activity, participants should be able to:

- describe the legal, clinical, financial and managerial issues pertinent to risk management;
- explain the impact of risk management issues on patients, physicians, nurses, legal counsel and management;
- identify solutions to risk management problems in healthcare for hospital personnel to use in overcoming the challenges they encounter in daily practice.

CNE INSTRUCTIONS

Nurses participate in this CNE program and earn credit for this activity by following these instructions.

1. Read and study the activity, using the provided references for further research.
2. Scan the QR code below, or log on to www.cmecity.com to take a post-test; tests are to be taken after each issue. First-time users will have to register on the site using the 8-digit subscriber number printed on their mailing label, invoice or renewal notice.
3. Pass the online tests with a score of 100%; you will be allowed to answer the questions as many times as needed to achieve a score of 100%.
4. After successfully completing the test, your browser will be automatically directed to the activity evaluation form, which you will submit online.
5. Once the completed evaluation is received, a credit letter will be emailed to you instantly. ✦

CNE QUESTIONS

1. What does John B. Rabun, ACSW, director of infant abduction response at the National Center for Missing & Exploited Children (NCMEC), say about security for older pediatrics in many hospitals?

A. It is not at the same level as security for newborns.
B. It is at the same level as security for newborns.
C. It is higher than security for newborns, which is appropriate.
D. It is higher than security for newborns but should not be.

2. On whom does South Nassau Communities Hospital, use security transponders to know when a patient is leaving the unit?

A. Newborns only
B. Newborns to 5 years old only
C. Any patient 17 and under
D. No one

3. What is one benefit of a hospital or health system using a captive to self-insure rather than a commercial insurer?

A. Money not paid out by the captive is retained by the healthcare provider.
B. Money paid to the captive is always 100% tax deductible.
C. The captive limits how much a plaintiff can be awarded.
D. Patients are less likely to sue if they know the provider is self-insured.

4. What does Jimmy Lin, vice president of product management and corporate development at The Network, suggest is an effective way to communicate with employees about social media restrictions?

A. An annual education session for all employees
B. Fliers and newsletters
C. Recorded phone calls
D. Short messages sent to them on social media

Legal Review & Commentary

Expert analysis of recent lawsuits and their impact on healthcare risk management

Surgical mistake leads to infection, loss of large intestine, and $12 million verdict

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

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

Tim Laquer,
2015 JD Candidate
Pepperdine University School of Law
Malibu, CA

News: The patient, a 65-year-old woman, sought treatment at a hospital for a hernia in 2008. During what was supposed to be a routine procedure to correct the hernia, the patient's colon was punctured. The operation was performed by an attending physician and a resident-in-training, which the patient was not informed about. The puncture was not detected at the time. Two days later, the patient's heart stopped. Along with the heart attack, the patient suffered from a serious infection, organ failure, and septic shock, which resulted in a month-long coma. The patient brought suit against the attending physician, the resident, and the hospital. She alleged that the physicians were negligent and the hospital was responsible for the activities of its resident training surgeon. Before the trial, the attending physician settled the claims against him, but the resident and hospital denied any wrongdoing. The jury found the resident and hospital liable and awarded the patient $12 million in damages.

Background: The patient was a 65-year-old grandmother who was suffering from a hernia and sought treatment at a hospital in 2008. She underwent what was supposed to be a routine laparoscopic procedure to correct the hernia, but during the operation, the patient's colon was punctured. While the patient was sedated, a member of the hospital's residency teaching program, who was not previously involved in the patient's case, was brought in to assist the attending physician in the operation. The patient did not know that a surgical resident would be taking part in her operation.

During trial, the testimony conflicted regarding what this resident actually did during the procedure. The surgical resident claimed that he performed only various surgical preparations and did not puncture the patient's colon, while the patient alleged that the attending physician allowed the surgical resident to use a special surgical device during the operation and he perforated the patient's colon. Regardless of which account is true, the patient's colon ultimately was perforated, and the perforation was not detected by the attending physician before the patient was closed.

As a result of the perforation, the patient developed a massive abdominal infection and subsequently suffered multiple organ failure, septic shock, and a heart attack, which necessitated urgent care to save the patient's life. She was rushed into an operating room, where the colon perforation was detected. Due to these severe complications, the patient required multiple surgeries to attempt to repair the damage done by the perforation. She went into a month-long coma as well. By the end of her inpatient treatment, the patient had spent 70 days in the hospital, lost most of her large intestine, and had accrued $1 million in medical bills. Her injuries resulted in her being unable to properly digest food and caused serious restrictions to her movement.

The patient brought suit against the attending physician, the resident (now a hand surgeon), and the hospital. She alleged that the physicians were negligent during the operation and that the hospital was responsible for the activities of its resident training surgeon. The patient claimed that the perforation of the colon, done by the resident, was action falling below the standard of care, and that the attending physician should not have allowed the resident to perform any surgical operations. Furthermore, her lawsuit alleged that the attending physician was

FINANCIAL DISCLOSURE: Author **Greg Freeman**, Executive Editor **Joy Daughtery Dickinson**, Nurse Planner **Maureen Archambault** and coauthors D**amain Capozzola**, **Jamie Terrence**, and **Tim Laquer** report no consultant, stockholder, speaker's bureau, research, or other financial relationships with companies having ties to this field of study.

negligent for not detecting the colon perforation before closing the surgical wound and finishing the procedure. Before trial began, the attending physician settled the claims against him, but the hospital refused to accept responsibility for its residents' program. At trial, the hospital argued that the individual physician was responsible for the acts of a resident, not the hospital itself. After three and a half hours of deliberation, the jurors agreed with the patient, found the hospital and resident jointly and severally liable, and awarded $12 million in damages.

What this means to you: Colon perforation is not an uncommon risk during any abdominal surgery and is seen more frequently in laparoscopic procedures than open laparotomies. Always ensure that the patient understands this risk and document that understanding in the medical record. That said, there was no issue regarding whether the patient suffered an injury caused by a physician falling below the standard of care in this case. The colon perforation was not debated, and such a mistake being overlooked and missed during an operation clearly constituted medical malpractice. The seriousness of the patent's injuries revealed just how much harm was caused by the missed perforation, and the defendants wisely did not attempt to argue this.

When the actions clearly fall below the standard of care, physicians and hospitals would be wise to do exactly what the attending physician did in this case: Settle before trial. Settlement has numerous advantages over proceeding all the way through with the case, and the most obvious of these is the amount of money to be saved. While verdicts can be expensive if unfavorable, they can be a relief if favorable; however, the verdict is a gamble. Even with helpful evidence, predicting a jury outcome can be difficult. Settlement, however, can eliminate this gamble and prevent huge jury verdicts. Settlement early also can prevent the drawn-out stress and costs involved with prolonged litigation. The case here was initiated in June 2010 and finally resolved at the end of May 2014. The attending physician here settled before the $12 million verdict and thus cannot be held liable for that amount, although the amount he agreed to pay was confidential.

The physician's negligence in this case was rather straightforward: The physician failed to properly oversee the surgical operation and failed to identify the punctured colon. Physicians have a duty to provide treatment that meets the applicable standard of care; that is, physicians must provide care that a reasonable physician would provide given the same or similar circumstances. There is nothing inherently wrong with allowing certain activities to be performed by other qualified medical staff, including nurses and residents, but the physician ultimately is responsible for the patient's treatment and must ensure that the correct steps have been taken. The standard procedural consent form always should state that the surgeon might have assistants including students and residents present during the procedure.

Although residents are licensed physicians, they still are students and in training. Residency programs must meet specific state and federal requirements for hospitals to receive funding from the government for providing the training. The requirements include strict resident oversight by qualified physicians and surgeons. This supervision is monitored and quantified by residency program leaders from the hospital and the school that provides the students. Results are reported to government agencies so that the hospitals can maintain their status as teaching facilities. The lack of oversight in this case might be attributed to the surgeon lacking enough information about the level of experience of the resident. It is not uncommon for a resident to be hesitant to tell an attending that he or she is unsure of a diagnosis or a procedure rather than being upfront and able to communicate openly. Much of this reluctance might be fear-based if attendings are insensitive to the needs of their students.

In any event, the attending physician in this case likely realized that he faced a difficult battle in arguing that he satisfied the standard of care when he completely missed a perforation in the colon during a routine hernia operation, especially considering that this perforation might have been the fault of someone under his own supervision. This case illustrates the point that physicians should be particularly cautious when delegating tasks to others, and make sure that these tasks were correctly performed, before finishing treatment procedures and discharging patients from their care. Failing to properly supervise procedures can lead to liability, when reasonable physicians given the same or similar circumstances would have a more active hand and adequately supervise such procedures.

Hospitals of all types can be held liable for the actions of their employees. Thus, they must be careful in properly supervising and creating procedures for oversight of such employees, which is an especially important point in jurisdictions and circumstances in which physicians are hospital employees instead of independent contractors. Teaching hospitals might have increased chance for liability based on the acts of their residents, as evidenced in this case. Residents themselves can and do get sued for medical malpractice, and they can be held to the same standard of care as fully licensed physicians. However, because plaintiffs likely will be looking for more and deeper pockets to pursue, an important question is who else can be responsible for the acts of the student.

There was a disagreement between the patient and the hospital as to who should be held liable when a resident-in-training acted negligently and whether this negligence should be imputed to the supervising physician or the teaching hospital. It is possible for either party to be held responsible. An attending physician can be held liable under a theory of vicarious liability, if the physician is present and fails to sufficiently supervise, or a theory of direct liability, if the physician fails to supervise as inherently required as part of the job position at a teaching hospital. Also, the hospital itself can be held directly liable. Hospitals have a duty to provide services and care to patients, and they have a duty to supervise that care. If a hospital's training program does not sufficiently provide for supervision, then the hospital itself might be liable for this failure. In an effort to protect themselves, hospitals should ensure that there are proper procedures and standards in place for physicians to follow in regard to their residents-in-

training.

Oversight and review boards can further assist these procedures to ensure that teaching physicians are properly supervising their students and making sure that the students don't exceed their experience or take on tasks for which they are ill prepared.

Reference

Superior Court of Danbury County, CT. Case No.DBD-CV10-6003939-S. May 30, 2014. ✦

Misdiagnosis leads to ruptured aneurysm — Survivor awarded $13.2 million

News: The patient, a 17-year-old man, presented at a hospital emergency department complaining of pain on and around his right eye in July 2010. At the hospital, he was seen by nursing staff and a physician assistant. The physician assistant diagnosed the patient with a form of conjunctivitis, commonly known as "pink eye." A supervising physician of the emergency department signed off on the physician assistant's diagnosis. The patient was given a prescription for antibiotics and discharged from the hospital within a few hours of being admitted. In November 2010, an aneurysm burst inside the patient's brain, which caused serious damage. The patient suffered serious, permanent brain damage as a result of the burst aneurysm. The patient's guardian brought suit against the physician assistant, the supervising physician, the hospital, and the hospital's staff service provider. All defendants denied any liability. The jury found the physician assistant, the supervising physician, and the hospital liable and awarded $13.2 million in damages.

Background: In this matter, the patient was a 17-year-old man who presented at a hospital emergency department complaining of pain on and around his right eye in July 2010. After being admitted to the hospital, the patient was attended to by nursing staff and a physician assistant. The physician assistant physically examined the patient and diagnosed him with a form of conjunctivitis, commonly known as "pink eye." A supervising physician responsible for the emergency department at the hospital approved of the physician assistant's diagnosis, but this approval was done without the supervising physician personally examining the patient. With this diagnosis approved, the patient was given a prescription for antibiotics and was discharged from the hospital only a few hours after being admitted while complaining of pain on and around his eye. No further testing was done to determine if a different condition caused the pain.

Four months later, in November 2010, the patient suffered a ruptured aneurysm. The patient was rushed to a facility for emergency surgery to treat the condition, but despite these attempts, he suffered serious injuries, including permanent brain damage as a result of the burst aneurysm. At the time of trial, the patient testified that he had trouble concentrating and remembering things, and he said he suffered from regular seizures. His description of the seizures to the jury was that it felt like "getting electrocuted and jumping like a fish on the floor." The patient permanently lost use of his left hand, walks with a cane, and his lawyers argued in court that he will require a life coach and caretaker for the rest of his life.

The patient's guardian brought suit against the physician assistant, the supervising physician, the hospital, and the hospital's staff service provider. Prior to trial, the hospital's service provider was dismissed from the case, but the remaining defendants remained.

The plaintiff alleged that the physician assistant's diagnosis was incorrect and, based on the patient's presentation in the emergency department, further testing was required to correctly diagnose his condition. Furthermore, according to the plaintiff, the supervising physician was negligent for failing to properly supervise the physician assistant and for approving the diagnosis without actually examining the patient.

During trial, the plaintiff had an emergency department expert testify that had the original physician assistant or supervising physician ordered a CAT scan and other appropriate testing, the condition could have been detected during the original July visit and the brain aneurysm could have been detected behind the patient's right eye. According to expert testimony, had this brain aneurysm been detected, treatment could readily have prevented it from bursting and causing the serious brain damage. Furthermore, expert testimony also stated that this action would have been the correct one to take, following the required standard of care for reasonable physicians given the circumstances. The defense's physicians attempted to argue that the proper treatment was given, according to the teen's presentation in the emergency department, which would not have caused a reasonable provider to do further testing.

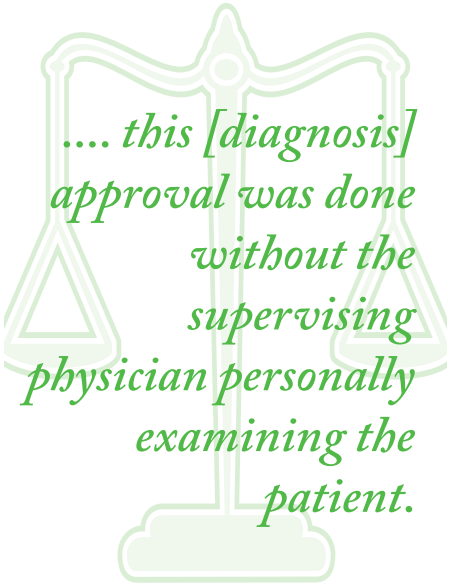
There were allegedly discrepancies with what the patient told the hospital staff at the time of the first examination. The hospital staff claimed that he reported eye pain, not head pain, and it was unclear which eye was in pain. The medical record showed that the pain was on the left side, while the patient claimed it was on the right, and a headache and eye pain can be caused by different conditions.

After a two-week trial, the jury mostly agreed with the plaintiff and awarded $13.2 million in damages. However, the jury partially agreed with the defense: It distributed liability equally among the physician assistant, the supervising physician, and the hospital at 30% each, in addition to 10% negligence on the patient for his discrepancies and inconsistent reporting to the hospital. This 10% negligence on the plaintiff reduced his overall award down to $11.88 million.

What this means to you: This case further illustrates the dangers inherent in the delegation of work within the medical field. While the previous case had an issue with a resident-in-training, this case had an issue with a physician assistant. Most urgent care centers and emergency departments use nurse practitioners and physician assistants in one or more capacity to support physicians. Physician assistants generally are considered licensed independent practitioners. The initial triage of patients as they enter a facility for urgent or emergent care usually will determine what level of provider will be assigned to the patient. The supervising medical staff organization of each facility is responsible for delineating the permissible activities and required supervision for each level of practitioner.

Although physician assistants are certified, licensed medical practitioners, they are not as qualified or specialized as a full physician, and this difference can create issues for liability among a practice group or within a hospital. States define differently the scope of physician assistants' practice, and most states require them to be under the direct supervision of a fully licensed physician. For example, in New Jersey, the Physician Assistant Licensing Act (PALA) limits the procedures that a physician assistant is authorized to perform, which includes gathering a patient's medical history, performing a physical examination, suturing and caring for wounds, and assisting a physician in inpatient rounds with the supervision of a physician.

Liability for the actions of physician assistants can be readily assigned to the hospital where the hospital employs the assistant and is responsible for the proper training and supervision of such assistants. Such hospitals, therefore, must ensure that physician assistants are allowed to perform only those activities as authorized by state law and that the assistants are properly trained and supervised by physicians. Similarly, training physicians regarding what are proper and improper activities for physician assistants to do will help to reduce liability of the hospital. Physicians



themselves must also be careful in delegating their important duties to those who are less qualified to perform them. As evidenced in New Jersey's rules, some states allow physician assistants to perform physical examinations of patients, but this situation should not increase the physician's reliance on such an examination. A physician who improperly relies upon someone else's examination and diagnosis, without objectively verifying the findings, does not satisfy his or her duty to provide the standard of care required by law.

In this case, the physician completely failed to examine the patient or verify the physician assistant's findings. This process does not need to be a long one. The physician could have read the assistant's findings and taken a few minutes to consult the patient herself. Even if the physician concurred with the assistant's finding of conjunctivitis, which was likely an improper diagnosis that the physician could have corrected, the mere fact that the physician examined and reached this conclusion would have greatly strengthened her defense during the trial. Over-delegation of duties can lead to liability because there are standards in place that require that a physician perform certain actions himself or herself. Failing to do so falls below the standard of care and constitutes medical malpractice.

While a complaint of eye pain accompanied by drainage, swelling, and other signs of obvious infection without high fever can be diagnosed and treated by a physician assistant in most cases, the additional complaint of a headache changed the required care. More generally, providers must accept the fact that there can be more than one pathology coexisting within a patient at the same time. We often see diagnoses and subsequent treatments based on superficial symptoms while underlying symptoms go unheeded. It is the garden path of least resistance that practitioners get led down. To avoid this, it is the provider's responsibility, regardless of level, to ask the right questions, and it is the patient's (and guardian's) responsibility to give the right answers.

Note that the defendants won a minor victory in this case by arguing that the patient himself was partially responsible for his own injuries. The jury found that the patient was 10% liable, and thus the overall damages were reduced by 10% on the theory of "comparative negligence." When a plaintiff is partially to blame, the damages are lessened by that same amount. This point can be a tricky one to argue, however, as a jury might perceive this to be a hospital or physician "blaming the victim." Stating that the (now) brain-damaged plaintiff is the cause of his own problems might not sit well with a jury, because the injured plaintiff is much more sympathetic than a hospital or physician. This case is an example of the tactic working well for the defense in that it reduced the overall damages award by 10%. This case justifies its limited use, according to the particular circumstances and rules of the jurisdiction. Different jurisdictions follow different rules regarding comparative negligence. Some jurisdictions follow an even harsher related regime of contributory negligence in which the defendant is barred from recovering if the defendant's own negligence plays any role in causing defendant's harm.

Reference

Pasco County Circuit Court, FL. Case No. 51-2011-CA-5035. Dec. 13, 2013. ✦

HIPAA Regulatory Alert
Cutting-edge information on privacy regulations

Physician's tinkering causes data breach, record $4.8 million in HIPAA settlements

Two prominent New York organizations have agreed to pay $4.8 million to settle charges stemming from a data breach, and they take the dubious honor of the largest settlement ever for violating the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. The breach has been traced to the actions of a single physician who had access to a computer server.

The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) says the providers failed to secure thousands of patients' electronic protected health information (PHI) held on their network. A major lesson from the breach is that partnering with another provider brings substantial risk if you do not thoroughly assess how data will be shared and protected.

OCR initiated its investigation of New York — Presbyterian Hospital (NYP) and Columbia University (CU) following their submission of a joint breach report, dated Sept. 27, 2010, regarding the disclosure of the PHI of 6,800 individuals, including patient status, vital signs, medications, and laboratory results. NYP and CU are separate covered entities that participate in a joint arrangement in which CU faculty members serve as attending physicians at NYP. The entities generally refer to their affiliation as "New York Presbyterian Hospital/Columbia University Medical Center."

NYP and CU operate a shared data network and a shared network firewall that is administered by employees of both entities. The shared network links to NYP patient information systems containing PHI. The breach did not happen in any of the most typical ways, such as a laptop being lost or stolen. Instead, a single physician mistakenly thwarted NYP and CU's security systems.

The OCR investigation revealed that the breach was caused when a physician employed by CU, who developed applications for NYP and CU, attempted to deactivate a personally owned computer server on the network containing NYP patient PHI. Because of a lack of technical safeguards, deactivation of the server resulted in PHI being accessible on internet search engines, the OCR reports. The entities learned of the breach after receiving a complaint by an individual who found the PHI of the individual's deceased partner, a former patient of NYP, on the internet.

In addition to the impermissible disclosure of PHI on the internet, OCR's investigation found that neither NYP nor CU made efforts prior to the breach to ensure that the server was secure and that it contained appropriate software protections.

"Moreover, OCR determined that neither entity had conducted an accurate and thorough risk analysis that identified all systems that access NYP PHI," OCR stated in announcing the settlement. "As a result, neither entity had developed an adequate risk management plan that addressed the potential threats and hazards to the security of PHI. Lastly, NYP failed to implement appropriate policies and procedures for authorizing access to its databases and failed to comply with its own policies on information access management."

Must assess risk of working with partner

NYP has paid OCR a monetary settlement of $3.3 million, and CU has paid $1.5 million. Both entities agreed to a substantive corrective action plan, which includes undertaking a risk analysis, developing a risk management plan, revising policies and procedures, training staff, and providing

EXECUTIVE SUMMARY

Two organizations will pay a combined $4.8 million to settle a case sparked by a breach of protected health information (PHI). The settlement is the largest ever for a violation of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

- The breach involved the PHI of 6,800 people.
- A physician caused the breach by accessing a server.
- Partnering with another provider brings substantial risk if you do not thoroughly assess how data will be shared.

progress reports. (The New York — Presbyterian Hospital Resolution Agreement may be found at http://tinyurl.com/lakqm96. The Columbia University Resolution Agreement may be found at http://tinyurl.com/ofyargl.)

The incident and the large settlement figure illustrate the risk that healthcare providers take on when working on such a data-driven project with another provider, says **Alisa L. Chestler**, JD, shareholder with the law firm of Baker Donelson in Washington, DC. "You have two entities here that were collaborating to do really good work, but even the most minute details of how you create, receive, transmit, or maintain information needs to be understood," Chestler says. "This employee of one essentially compromised them both by trying to terminate access in a way that obviously didn't work. This shows that you have to ask what you know about what your partner is doing and how they're doing it."

A thorough risk analysis is necessary for any partnership involving data sharing, Chestler says. Both of the corrective action agreements in this case call for a risk analysis.

Risk analysis failure can be your downfall

The risk analysis failure turned out to be as important to this case as the breach itself, which did not involve as many patients as some previous breaches, says **Brad Rostolsky**, JD, an associate with the law firm of Reed Smith in Philadelphia. One sure lesson from the New York case is that you want to stay out of the government's way as much as possible, he says. Once OCR investigated the breach, it found overall deficiencies in HIPAA compliance.

"If they look at you for HIPAA compliance purposes and determine that you have not conducted an appropriate risk assessment under the security problem, there's going to be a problem," Rostolsky says. "Notwithstanding everything you may be doing with HIPAA compliance, if you have not conducted an appropriate risk assessment, you are going to be in trouble if the government finds out."

A key term there is "appropriate." OCR investigators will not look kindly on a risk analysis that seems perfunctory or trying to meet minimum expectations, Chestler says.

"Your risk analysis cannot be a 'check-the-box-and-move-on' exercise," she says. "You may be working with a partner that has a stellar reputation and you have every reason to think their data security plan is top notch, but you still have to go through the due diligence of looking at how data is handled. I'm sure in this case both parties thought they had adequate controls, but there was a fault in the system."

Chestler sees still another message in the New York settlement. OCR is pursuing HIPAA violations with vigor in a wide range of healthcare settings, from small government entities to huge private sector companies such as Wellpoint and these New York entities, she notes. "They are clearly trying to send a message that they are taking a broad approach to enforcement so that no one, large or small, starts to feel that they are under the radar," Chestler says. "There are going to be a lot more settlements like this one. Whether you're a big system or a small provider, nobody is immune."

OCR is becoming more aggressive in enforcing HIPAA and the hopscotching from private to government entities, big to small, is making their actions hard to predict.

Interestingly, the resolution agreements call for more specific training of employees and physicians, Chestler says. She sees that as a warning that OCR is expecting more detailed training tailored to your own organization rather than generic HIPAA education. "I don't think those off-the-shelf HIPAA education programs are going to work anymore," she says.

SOURCES

• **Alisa L. Chestler**, JD, Shareholder, Baker Donelson, Washington, DC. Telephone: (202) 508-3475. Email: achestler@bakerdonelson.com.
• **Brad Rostolsky**, JD, Associate, Reed Smith, Philadelphia. Telephone: (215) 851-8195. Email: brostolsky@reedsmith.com. ■

Desk audits are coming, but what are they like?

The Department of Health and Human Services (HHS) Office of Civil Rights (OCR) will begin conducting desk audits for Health Insurance Portability and Accountability Act (HIPAA) compliance this fall, which has many providers wondering just what they will be like. Most HIPAA experts expect the desk audits to be relatively pain-free, but until someone goes under the microscope, no one can be sure.

OCR is selecting a sample of covered entities, which includes hospitals and other medical service providers, to perform desk audits. OCR has started contacting 500-800 covered entities in preparation to survey these entities this summer. From that 500-800 entity survey group, OCR is going to select 350 covered entities on which to perform desk audits. Some hospitals will be

included. The HIPAA desk audits start in October 2014, and they will run until June 2015.

The hospitals won't receive notice that they are getting a desk audit until late summer or early fall of this year. The desk audits represent phase two of OCR's HIPAA audit program, notes **Melissa Goldman**, JD, an attorney with the Florida Health Law Center in Davie. Phase one, which began in 2012, involved full on-site audits for covered entities conducted by the outside accounting firm KPMG, but the desk audits will be much narrower, more targeted, and conducted by OCR, Goldman says. OCR also will audit some business associates of each provider audited, she says.

So how will the desk audits be conducted? The term "desk audit" is intended to convey that the audit will not be an on-site visit, but rather providers should be able to respond to the audits from their desks by providing policies and documentation of privacy policies and procedures, explains **Patricia Wagner**, JD, an attorney with the law firm of Epstein Becker Green in Washington, DC. For organizations that are well-organized, the response process should be relatively pain-free, she says. Rather than an on-site visit during which the auditors would interview employees about HIPAA compliance, the desk audit is strictly a look at documentation. That difference means that you won't have to tie up a lot of employee's schedules with time to meet personally with auditors.

"Providers should ensure that their privacy policies and procedures reflect the compliant privacy and security practices of the organization," Wagner says. "Providers won't have the opportunity, as they might in an on-site audit, to describe a process that takes place that may not be otherwise documented."

The inability to explain anything lacking or unclear in the documentation will put some organizations at a disadvantage, Goldman says. "The documentation will speak for itself, whether that is good or bad," she says. "If your documentation is such that you're compelled to explain what isn't there on the page, or why you didn't write something exactly in the way the statute requires, you may be in trouble."

For that reason, risks managers and compliance officers should assess their documentation now, before it is requested in an audit, Goldman says. In addition to having all the required policies and procedures, you should ensure that there are no privacy notices that have not been signed and that you have a system for tracking compliance.

Third-party risk management will be a major focus of the desk audits because it is now required in the statute, notes **Michael D. Ebert**, JD, partner with the accounting and consulting firm of KPMG in Philadelphia. Ebert led the work to develop the HIPAA audit program for the government. In this area, auditors will be looking at how the provider or associate is protecting health information and whether it is meeting the protocol requirements of the security rule, he says. *(See the story on p. 4 for more tips on surviving a desk audit.)*

"In the initial audits, two-thirds of the findings were in security, but only one-third of the test procedures performed were in security," Ebert says. "That's why OCR has said they are going to focus more on the security rule than in the privacy rule. This time they're reversing it so that two-thirds of the testing will be about security, and one-third will be about privacy."

To that end, auditors are likely to look at whether providers are training employees on HIPAA compliance and making them aware of the security and privacy rules. This auditing might cover everything from annual training programs to placards in elevator lobbies reminding employees not to talk about PHI in common areas.

Goldman suspects one area of interest will be risk assessments, which were the weak points in many phase one audits. She cautions that conducting a proper assessment is not enough; you must also provide adequate documentation of the assessment, agrees Ebert, noting that in his experience, 90% of risk assessments do not meet OCR's standards. One reason is that most risk assessments are performed internally rather than by an independent evaluator, he says.

If the risk assessment or any other significant component is inadequate, the desk auditors could refer the provider for a live on-site audit, Ebert explains, and that step opens up the possibility of finding many more deficiencies. Fines also can be assessed without an on-site audit.

Device security might be examined

Goldman also expects OCR to look at device security.

"Are your computers password protected, at a minimum? Are you sending email with encryp-

EXECUTIVE SUMMARY

The Department of Health and Human Services (HHS) Office of Civil Rights (OCR) will begin conducting desk audits for compliance with the Health Insurance Portability and Accountability Act (HIPAA) in October 2014. These audits will be conducted remotely by requesting compliance documentation.

- Adequate and updated risk assessments will be one focus.
- Providers will not have the opportunity to explain any documents.
- Auditors will look closely at compliance with the security rule.

tion?" she says. "I think encryption might be more of an issue with the 2015 and 2016 audits, but it's entirely possible they will inquire about this year. If it is not encrypted, do you have documentation showing that you informed the patient of that and the patient agreed to receive the email anyway?"

Expect follow-up requests and questions after supplying the material requested initially, **Jorge Rey**, CISA, CISM, CGEIT, director of information security and compliance with the accounting firm Kaufman Rossin, based in Miami. Be responsive and transparent, but also think about what you're sending, he says.

A primary goal should be helping the auditor understand what you are sending and how it is responsive to the documentation request. Don't send a batch of documents and let the auditor sort out what they are.

"You can always put your best foot forward," Rey says. "If the auditor requests policy A, send that information with a cover noting that this is policy A, in response to your request on whatever date. Provide that information in the way that makes it as easy as possible for the auditor. No one likes going through an audit, but if you help the auditor, the auditor may be able to help you as you're going through the process."

Ebert, with his extensive experience working with the earlier HIPAA audits, says providers and their business associates should take the desk audits seriously. The fact that they involve only documentation and not on-site visits should not lead to complacency, he says. "I suspect a lot of covered entities will not meet the requirements of a desk audit," he says.

SOURCES

• **Jorge Rey**, CISA, CISM, CGEIT, Director of Information Security and Compliance, Kaufman Rossin, Miami. Telephone: (305) 646-6076. Email: jrey@kaufmanrossin.com.
• **Patricia Wagner**, JD, Epstein Becker Green, Washington, DC. Telephone: (202) 861-4182. Email: pwagner@ebglaw.com. ■

Update risk assessments, don't comply on the spot

An initial risk assessment will not enough when you undergo a desk audit, says **Bruce D. Lamb**, JD, a shareholder with the Gunster law firm in Tampa Bay, FL. Risk assessments should be conducted on a periodic basis, with proper documentation, he says. Any breaches of data security must be fully explained, with documentation that details how it was discovered, how affected parties were notified, and any corrective action taken, Lamb says.

"There were some pretty significant changes made in the notification requirements, so obviously if you haven't updated your policies and procedures to keep up with the changes that will be problematic for some entities," Lamb says. "Auditors also will look at how you are classifying classes of employees who have access to data and who doesn't, along with organizational charts."

There also should be documentation that a security official or committee has been designated and when. As with other points of compliance, the date it happened can be crucial.

"In the earlier phase, there were circumstances where the documentation was requested, and then people were rushing to fix the problem before responding," Lamb says. The Department of Health and Human Services Office of Civil Rights "is on to that, and they will be looking not only at whether you complied. Backdating things or complying on the spot is not going to work very effectively." ■

Google Glass could become HIPAA-compliant

Google Glass, the eyeglass-like device that provides constant computer access, takes photographs, and streams live video, has been used during surgery at some facilities, but there have been questions about whether some uses would violate the Health Insurance Portability and Accountability Act (HIPAA). A new partnership with a software company might help reduce that risk.

CrowdOptic, a company in San Francisco, CA, that makes video streaming software for wearable devices, recently announced a partnership with the University of California, San Francisco (UCSF) to develop ways to use the device in medicine. A key step will be including software that allows the surgeon to stream video to a local server instead of Google's server, as is normally done.

Sending the video stream to a local server will allow the healthcare provider to restrict who has access to protected health information (PHI), the company says. Some of the Glass features will be unavailable in this mode, but the surgeon can switch back to normal mode when compliance is no longer necessary, the company says.

If the device can be made HIPAA-compliant, CrowdOptic and USCF researchers say Glass might be used much more widely in the OR. ■