Healthcare Risk Management™

AHC Media LLC

IN THIS ISSUE

Financial Disclosure: Author Greg Freeman, Managing Editor Karen Young, Associate Publisher Russ Underwood, 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.

FEBRUARY 2010
VOL. 32, NO. 2 • (pages 13-24)

Feds may increase enforcement with HITECH, seek high penalties

Large penalties could be used as leverage in fraud and abuse cases

After one year of HITECH, risk managers are realizing that this rule is serious business. The stakes are higher, and there is reason to believe that federal prosecutors will use HITECH more aggressively in 2010 than they did during its first year.

The Health Information Technology for Economic and Clinical Health Act, known as HITECH, was enacted as part of the American Recovery and Reinvestment Act of 2009 and modified the Health and Human Services secretary's authority to impose civil monetary penalties for violations under the Health Insurance Portability and Accountability Act (HIPAA) occurring after Feb. 18, 2009. HITECH significantly increased the penalty amounts the secretary may impose for violations of the HIPAA rules.

Prior to the HITECH Act, the secretary could not impose a penalty of more than $100 for each violation or $25,000 for all identical violations of the same provision. A covered health care provider, health plan, or clearinghouse also could bar the secretary's imposition of a civil monetary penalty by demonstrating that it did not know that it violated the HIPAA rules. Section 13410(d) of the HITECH Act strengthened the civil monetary

EXECUTIVE SUMMARY

The HITECH rule poses a high risk for health care providers who run afoul of privacy laws. Some analysts predict that the federal government will pursue violations more vigorously now that multimillion-dollar penalties are possible.

- U.S. attorneys may see HITECH as a way to generate revenue for a cash-strapped government.
- Risk managers should conduct formal and informal audits to monitor compliance.
- Paper records often are the source of privacy breaches.

penalty scheme by establishing tiered ranges of increasing minimum penalty amounts, with a maximum penalty of $1.5 million for all violations of an identical provision. A covered entity can no longer bar the imposition of a civil monetary penalty for an unknown violation unless it corrects the violation within 30 days of discovery.

What does all this mean for risk managers? Nothing good. With the passage of HITECH, the federal government upped the penalties for breaches of security and privacy, but the legislation also put them in tiers, explains **Lisa L. Dahm**, JD, LLM, health director of continuing legal education and adjunct professor at the South Texas College of Law in Houston.

"So, not only is there now a higher risk because of the penalties that can be associated, but the conduct itself has changed," she says. "It used to be that if you just kind of ignored HIPAA and didn't feel like complying, you would be penalized the general amount, $100 per violation up to a maximum of $25,000 per calendar year. Now, there are levels of penalties and culpability."

For simple "did-not-know" errors, honest mistakes, the standard penalty still is $100 for each identical violation, Dahm says. So, if you make the identical error — such as entering the wrong code — on 20 claims, that still will count as one violation. The scary part comes when you're penalized for multiple violations or if your error wasn't so benign.

Under HITECH, health care providers are held accountable for the nature of the error, she says. HITECH exacts higher penalties for willful neglect, as opposed to making an honest mistake, she says.

"This signals that, with everything going on now with health care, one of the ways that the government is trying to pay for that is through the increased sanctions," Dahm says.

Better investigators now

Dahm says the government is targeting health care providers much more now than in the past. She used to tell health care providers not to panic if government agents came looking at their medical records, because, in most cases, the investigators didn't really know what they were looking for.

"Now they do, because for the past 10 years the government has been hiring people who have the knowledge, the billers and coders who know where to look," she says. "Now, when they ask for your records, it's not an FBI agent who hardly knows what he's looking at. It's a former coder or biller who is going to know exactly what to look for."

In addition to fraud and abuse, Dahm suspects that prosecutors will pursue HIPAA violations more aggressively than in the past, partly because the potential penalties are higher and that can be used as a bargaining chip.

"There is reason to think that the government is going to go after HIPAA violations as seriously as it does fraud and abuse," she says. "We're going to see U.S. attorneys saying they'll find you guilty of $400 million worth of fraud and abuse, and they'll toss in another $1.5 million of HIPAA violations.

Healthcare Risk Management® (ISSN 1081-6534), including **HRM Legal Review & Commentary**™, is published monthly by AHC Media, LLC, 3525 Piedmont Road, Building Six, Suite 400, Atlanta, GA 30305. Telephone: (404) 262-7436. Periodicals Postage Paid at Atlanta, GA 30304.

POSTMASTER: Send address changes to ***Healthcare Risk Management***®, P.O. Box 740059, Atlanta, GA 30374.

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., one year (12 issues), $499. Add $17.95 for shipping & handling. Outside U.S., add $30 per year, total prepaid in U.S. funds. For approximately 15 CE nursing contact hours, $545. 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.)

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.

Editor: **Greg Freeman**, (770) 998-8455.
Director of Marketing: **Schandale Kornegay**.
Managing Editor: **Karen Young** (404) 262-5423 (karen.young@ahcmedia.com).
Associate Publisher **Russ Underwood** (404) 262-5521 (russ.underwood@ahcmedia.com).
Senior Production Editor: **Nancy McCreary**.

Editorial Questions

For questions or comments, call **Greg Freeman**, (770) 998-8455.

Then, they'll offer to throw out the HIPAA violations and hold fast on the fraud and abuse. That's their leverage as a U.S. attorney. They haven't done that yet, but now it makes sense."

Dahm notes that the tactic will be easy to employ, because virtually every covered entity is in violation of HIPAA at some point.

"Not because they want to, but just because it happens," she says. "People don't necessarily intend to submit a false claim either, but it just slips through sometimes. Fortunately, under the fraud and abuse laws, you have to knowingly commit fraud to incur a big penalty. Under HIPAA, you don't have that protection." **(State attorneys general also can enforce HIPAA and employ HITECH penalties. See the story, p. 17, for more information.)**

Reaching out to the IT department is a good idea, Dahm says. Don't assume they know what they're doing when it comes to HITECH compliance or that they understand the size of the potential penalties. Business associates also can put the health care provider at risk if they fail to comply. **(See p. 16 for more on business associates' understanding of HITECH.)**

HIPAA is being used more to punish the criminal mismanagement of information, says **Robert D. Belfort**, JD, a partner with the law firm Manatt Phelps in New York City. The HITECH provisions have been used in the past year against intentional misuse of information, and Belfort says it is important for risk managers to be able to separate the health care provider from such egregious acts.

"The risk manager must establish compliance programs that position them to show that individuals were acting outside their training, authority, and direction, so that the institution won't be held responsible criminally and the penalties will be imposed only on the individual," he says. "So far, we haven't seen any criminal cases where the companies have been charged, and I think that is because the organizations involved were able to show that they are providing training; and the actions of the individual were not reflective of the organization's culture on the whole and, in fact, violated express directions given to the employee."

To make that case, the health care provider must have a solid paper trail showing that the employee was properly trained and that the incident does not signify a systemic problem in the organization.

"The organizations that avoided criminal prosecution were able to show that the behavior was very much at odds with their organization's culture and standards," he says.

HITECH is a powerful enforcement tool, but it can be used against even the simplest violation, so don't forget that privacy breaches don't have to involve a high-tech scenario. The high penalties possible with HITECH were aimed mostly at willful or egregious privacy breaches, such as the loss of a laptop computer with thousands of unprotected files, says **Pamela E. Hepp**, JD, an attorney with the law firm Buchanan Ingersoll in Pittsburgh, but old-fashioned paper often is the culprit.

Most HIPAA violations are on a small scale, with one patient involved, she says.

"The cases often are related to providers still using paper records and the piece of paper being misplaced and falling into the wrong hands, or perhaps bad behavior by employees accessing records that they shouldn't have," Hepp says. "There is a lot of emphasis on electronic security and encryption, but there are still a lot of instances in which paper records are not being protected adequately." ■

SOURCES

For more information on HITECH compliance, contact:

- **Robert D. Belfort**, JD, Partner, Manatt, Phelps & Phillips LLP, New York City. Telephone: (212) 830-7270.
- **Lisa L. Dahm**, JD, LLM, Health Director of Continuing Legal Education and Adjunct Professor, South Texas College of Law, Houston. Telephone: (713) 646-1873. E-mail: ldahm@stcl.edu.
- **Pamela E. Hepp**, JD, Counsel, Buchanan Ingersoll & Rooney PC, Pittsburgh. Telephone: (412) 562-1418. E-mail: pamela.hepp@bipc.com.

Past compliance efforts may not be enough

The substantial penalties possible with HITECH are good reason for risk managers to take a fresh look at their HIPAA compliance programs, says **Alisa L. Chestler**, JD, an attorney with Baker Donelson in Washington, DC. It has been many years since most HIPAA compliance programs were initiated, and the outlook on HIPAA compliance and enforcement has changed since then, she says.

SOURCE

For more information on reviewing HIPAA compliance, contact:

- **Alisa L. Chestler**, JD, Of Counsel, Baker Donelson, Washington, DC. Telephone: (202) 508-3475. E-mail: achestler@bakerdonelson.com.

"Risk managers need to take a step back, take a deep breath, and look at the direction of their plans and whether they are fully integrated into all facets of their operations," Chestler says. "For example, you may not have had a particular line of operations when HIPAA went into effect, and when you adopted that line, did you integrate that fully into your HIPAA compliance plan? You may have given it a close inspection regarding HIPAA at the time you took on that line of operation, but did you fully incorporate it into all aspects of your compliance effort?"

Chestler generally advises focusing more on compliance than the details of the HITECH enforcement options, because, after all, the goal is not to get to the point of penalties. But at the same time, she says, risk managers must be able to defend against a claim of willful neglect, which would bring the harshest penalties.

"You must be able to show good evidence that you've been doing your due diligence all along, and that isn't just writing a policy and putting it on a shelf," she says. "Your work is never done. If you wrote a solution for a situation a few years ago, you need to go back and see if that solution is actually working."

Lisa L. Dahm, JD, LLM, health director of continuing legal education and adjunct professor at the South Texas College of Law in Houston, advises risk managers to continuously monitor compliance. Formal audits are necessary, but spot checks of billing, medical records, policies, and procedures also are vital to ensure compliance, she says.

"Audits don't have to be a big deal with statistically significant sample sizes and a complex analysis," she says. "It can be as simple as the risk manager spending some time in the ER and watching what happens to see if people are disclosing health information when they shouldn't be. It can be walking into the medical records department to see how they handle records requests. An audit can be going up and down in the same elevator for an hour to see how people are talking about patient information." ■

Many vendors not ready for HITECH compliance

Vendors may be the Achilles heel of HITECH compliance, says **L. Elise Dieterich,** JD, a partner with the law firm Sullivan & Worcester in Washington, DC. "The important point here is that the HITECH amendments to HIPAA extended the rules and penalties that previously applied only to health care providers, to many of their vendors, as well," she says. "This means that both health care providers and all of their vendors that handle or have access to patient information should be revisiting their contracts to ensure that the contracts allocate the risk and responsibility associated with HIPAA compliance."

A key issue for providers implementing practice management systems and, in particular, electronic medical records, will be ensuring that their software provider and other vendors are fully compliant with HITECH, Dieterich says.

"Specifically, health care providers and their vendors now share responsibility — and liability — for any breach of confidentiality of patient information handled in electronic form," she says. "Health care providers must ensure by contract that their business associates meet the HITECH Act's expanded HIPAA requirements."

They may not be ready. Many business associates, that is, those who handle private patient information for health care organizations, are largely unprepared to meet the new data breach-related obligations included in the HITECH Act, according to the results of a survey by HIMSS Analytics, a not-for-profit subsidiary of the Healthcare Information and Management Systems Society (HIMSS) in Chicago.

Business associates can include everyone from billing, credit bureaus, benefits management, legal services, claims processing, insurance brokers, data processing firms, pharmacy chains, accounting firms, temporary office personnel, and offshore transcription vendors. The HIMSS Analytics research revealed that about one-third of business associates surveyed were not aware that they need to adhere to federal HIPAA privacy and security requirements. But the survey also revealed that health providers are taking action:

- 85% of health providers said they will take steps to ensure that data held by business associates will not be breached.
- Nearly half of hospitals, 47%, said they

would actually terminate their contracts with their business associates for violations.

"Business associates could represent a risk to health care organizations, especially hospitals," says **Lisa Gallagher**, BSEE, CISM, CPHIMS, senior director, privacy and security for HIMSS. "The lack of awareness of new federal regulations by business associates, coupled with the large number of third parties hired by hospitals to control costs through outsourcing, points to a potential area of concern. Hospitals, in partnership with their business associates, need to actively prepare to comply with the new rules when these breaches happen."

The research also found that:

- 50% of large hospitals experienced at least one data breach this year;
- 68% of all hospitals indicated that the HITECH Act's expanded breach notification requirements will result in the discovery and reporting of more incidents, and 57% reported that they now have a greater level of awareness of data breaches and breach risk;
- 90% indicated they have changed or plan to change policies and procedures to prevent and detect data breaches.

HITECH leaves some thorny questions about business associates unanswered, says **Glen Day**, CISSP, CISM, a principal with the consulting firm of Booz Allen Hamilton in Los Angeles and the former chief privacy officer for Los Angeles County during the initial implementation of HIPAA. For instance, the law says business associates who suffer a privacy breach must report that to the health care provider, and the provider, because it has the primary relationship with the patient, is responsible for reporting the breach to the government and notifying patients.

"They don't say who's supposed to pay for that. So, is the hospital going to be on the hook when the associate caused the breach?" Day says. "Is the hospital going to have its brand damaged because of what a third-party contractor did? If risk managers aren't looking at the true risk of associates mishandling data, you probably won't write the contract with sufficiently strong language."

Day advises including contract provisions that make the associates responsible for any liability resulting from a breach. Demand this protection up front, because once a breach happens, the provider is obligated to notify patients, regardless of whether you are successful in trying to get the associate to do the right thing, Day says.

Risk managers also must be on the lookout for some tricky parts of HITECH, Day says. For instance, HITECH provides a safe harbor for the accidental release of information that was encrypted, so a data breach doesn't necessarily mean a privacy breach if that information was encrypted so as to make it useless to another party.

"But how is it encrypted? Is it encrypted with some simple password that can be broken by anyone with some simple tools in a matter of minutes? Was it encrypted using high-end technology that you can trust won't be broken?" Day says. "The government tells you what to do — but not how well to do it. So, providers need to take ownership of how well they need to do it, based on existing risks, existing threats, and how you do your business." ■

SOURCES

For more information on HITECH risks from vendors, contact:

- **Glen Day**, CISSP, CISM, Principal, Booz Allen Hamilton, Los Angeles. Telephone: (310) 297-2120. E-mail: Day_glen@bah.com.
- **L. Elise Dieterich,** JD, Partner, Sullivan & Worcester, Washington, DC. Telephone: (202) 370-3925.

Watch for interstate patients and enforcement

Because HIPAA can be enforced by state attorneys general and not just the feds, risk managers should study any interstate connections that could come into play if there is a privacy breach, advises **Christine G. Leyden**, RN, MSN, vice president and general manager for client services, and chief accreditation officer with URAC, an independent, nonprofit organization in Washington, DC, that promotes health care quality through its accreditation and certification programs.

A large hospital system may serve consumers from different states, for instance, and that would expose the provider to enforcement action from all of those states, Leyden says. Furthermore, it is important to know exactly where in that state the patient lives, because the attorney general in one may handle HIPAA cases differently than the attorney general in another.

This strategy may be new to many risk managers, who are used to dealing only with their

SOURCE

For more information on state authorities enforcing HIPAA, contact:

- **Christine G. Leyden**, RN, MSN, Vice President, General Manager for Client Services, Chief Accreditation Officer, URAC, Washington, DC. Telephone: (202) 216-9010.

own state authorities. The significant penalties available under HITECH may make interstate enforcement appealing to attorneys general, Leyden says, and each attorney general has a different style and history of enforcement.

"Depending on the attorney general in . . . that state, you may have a very different experience when there is a breach," she says. "You may want to draw up a road map showing where your patients are from and contact that attorney general for guidance, and attend any meetings or advisory groups they offer as they roll out their enforcement." ■

Choice of tool can lower risk of airway fires

About 650 surgical fires are reported in U.S. hospitals each year, according to the nonprofit ECRI Institute in Plymouth Meeting, PA, and there are another three to four times as many near-misses. Fires during surgery can be extremely serious, causing significant injuries and death to both patients and clinicians.

Risk managers can reduce the risk of surgical fires by encouraging safe practices, including the careful choice of instrumentation that is less likely to contribute to a fire, suggests **Soham Roy**, MD, associate professor at the University of Texas Medical School at Houston in the Department of Otorhinolaryngology — Head and Neck Surgery. He also is director of pediatric otolaryngology — Head and Neck Surgery at Children's Memorial Hermann Hospital in Houston.

The Joint Commission has recognized the threat of surgical fires, releasing a *Sentinel Event Alert* in 2003 that outlined strategies to prevent surgical fires.[1] In that *Alert,* The Joint Commission noted that electrosurgical equipment sparks the most fires (68%), followed by lasers (13%). The airway is the most common location of fire (34%), followed by face and head (28%), and elsewhere inside or outside the patient (38%); an oxygen-enriched atmosphere contributes to 78% of all cases.

Roy has studied the issue extensively and says the risk of surgical fires may be worse than the statistics indicate.

"A lot of people fail to understand just how serious this problem is. Surgical fires are probably one of the most underreported phenomena in the operating room," Roy says. "Surgical fires are considered a never event, and people think this is an isolated incident that happens once a year around the country, and it's never going to happen to you."

Fires occur with surprising regularity in some specialties. Roy and a colleague recently surveyed members of the American Academy of Otolaryngology — Head and Neck Surgery on their experience with surgical fires and found that 25% of respondents had personally witnessed at least one fire in the operating room. Interestingly, 10 people reported being involved with two fires, and two surgeons reported five fires apiece. **(For a recent example of how a surgical fire occurred, see p. 19.)**

"It's more common than you think, but it's rarely discussed," Roy says. "People think of it as a once-in-a-lifetime event, but it can happen a lot more than once in a lifetime."

Roy's research suggests that the risk can be significantly reduced by choosing surgical tools less likely to start a fire. He conducted a study that demonstrated the risk factors of various surgical modalities, including electrocautery (Bovie), CO_2 laser, and Coblation (bipolar radiofrequency ablation) over the past two years.[2] In his research, Roy and his colleagues examined the risk of fires and

EXECUTIVE SUMMARY

Airway fires are a serious threat to patient safety during surgery, and recent research suggests that the type of tools used can significantly affect the risk level. Risk managers can mitigate the risk by encouraging clinicians to consider fire prevention when determining treatment options.

- Surgical fires are not as rare as many people think and may be underreported.
- Coblation tools may pose less risk than electrocautery and CO_2 lasers.
- Surgical teams should discuss the risk of fire before each procedure.

burns during endoscopic surgeries with halogen light sources, electrosurgery, and created mechanical chicken models to study fire risk in oropharyngeal and airway surgeries. The research determined that the Coblation eliminated the risk of surgical fire, as it produces less thermal energy dissipation with lower surrounding temperatures in the tissues, which eliminates the ignition source necessary to spark a fire. Even in a 100% oxygen-enriched environment, the risk of surgical fire was eliminated in Roy's model using Coblation, he says.

Roy explains that head and neck procedures are at the highest risk of surgical fire, due to the presence of exposed supplemental oxygen around flammable materials. Fires have been reported during tracheostomy, adenotonsillectomy and skin surgery of the head and neck.

No matter where they occur, surgical fires require a "classic triad" of elements to occur: an ignition source, fuel, and an oxidizer. Ignition sources often are electrosurgical units, lasers, and light cords; and endotracheal tubes, operating room drapes or towels, sponges and alcohol preparation solutions can provide the fuel. The oxidizing agent can be a gas commonly used in surgery, such as oxygen or nitrous oxide.

The role of oxygen and nitrous oxide are important factors to consider. Roy recommends that the anesthesiologist collaborate with all surgical team members throughout the procedure to minimize the presence of an oxidizer-enriched atmosphere in proximity to an ignition source. Keeping the fraction of inspired oxygen (FiO_2) below 50% may eliminate the risk of fire ignition, he says.

Surgical fires can be small and quickly controlled, but they also can be fatal. Janice McCall, a 65-year-old woman from Energy, IL, died Sept. 8, 2009, at Vanderbilt University Medical Center in Nashville, TN, six days after being burned on the operating table at Heartland Regional Medical Center in Marion, IL, according to her family attorney, **Robert Howerton**, JD, of the law firm Howerton Dorris in Marion, IL.

The Tennessee state medical examiner's office said McCall died from complications of thermal burns and classified her death as accidental. Heartland released a statement confirming that "there was an accidental flash fire in one of the hospital's operating rooms," which was immediately extinguished but injured the patient.

"Awareness is the key to prevention. Once you convince people that this is a real risk, there are steps to take and ways to greatly reduce that risk," Roy says.

SOURCES

For more information on preventing surgical fires, contact:

- **Robert Howerton**, Partner, Howerton Dorris & Stone, Marion, IL. Telephone: (618) 993-2616. E-mail: rhunter@neondsl.com.
- **Soham Roy**, MD, Director of Pediatric Otolaryngology — Head and Neck Surgery, Children's Memorial Hermann Hospital, Houston. Telephone: (713) 704-5437.

Roy urges risk managers to employ policies and procedures that can reduce the risk of fire. Before each surgical case, he says the OR team should consider whether the case is at high risk for surgical fires — determined by the procedure, materials, and gasses in use, and the instrumentation. If those factors suggest a high risk, the team should decide on a plan for preventing and managing a fire. This could all be discussed during the timeout before surgery, he suggests.

Communication between nursing staff, anesthesiologist, and surgeon is critical, Roy says.

"Fires tend to occur when there is miscommunication or a lack of communication [among] surgeons, anesthesiologists, and operating room staff," he says. "It is incumbent that everyone, not just the surgeon, realize there is a risk of fire and that the entire team communicates openly about how they're going to prevent it from happening."

References

1. The Joint Commission. Preventing Surgical Fires. *Sentinel Event Alert*; Issue 29, June 24, 2003.

2. Roy S, Smith LP. "Device-Related Risk of Airway Fire in Oropharyngeal Surgery." Abstracts of the AAO-HNS Annual Meeting, 2008; *American Journal of Otolaryngology*. ■

Patient catches fire during organ surgery

A recent example of a surgical fire reported by **Mary A. Herman**, MD, PhD, assistant professor of anesthesiology at the University of Florida College of Medicine in Gainesville, illustrates how such an incident can occur in routine circumstances.

Herman reports that the case involved a 19-year-old man who suffered severe head trauma

SOURCES

For more information on this case, contact:
- **Mary A. Herman**, MD, PhD, Department of Anesthesiology, University of Florida College of Medicine, Gainesville. Telephone: (352) 265-8012. E-mail: mherman@anest.ufl.edu.

and multiple injuries in a motor vehicle accident.[1] After he was declared brain dead at Shands Hospital at the University of Florida, clinicians began an organ procurement procedure. The donor was ventilated with a 32% oxygen/air mixture, and the donor's oxygen saturation (SpO_2) was 100%. A transplant surgeon cleaned the thorax and abdomen with alcohol, and a purulent discharge around the tracheostomy site was also removed with alcohol. The surgeon then wrapped a soaked, gauze sponge around the tracheostomy tube and left it in place. The donor was then aseptically prepared from sternal notch to pelvis with iodine povacrylex and isopropyl alcohol, which dried before the body was draped with cloth towels and paper drapes.

About 15 minutes after incision using an electrocautery device, the surgeon exclaimed that the donor was on fire. The anesthesiologist immediately disconnected the breathing circuit from the anesthesia machine and turned off all gases. The surgeon used a towel in an attempt to smother the flames, but the fire spread quickly to the drapes. The circulating nurse left the room to find water or a fire extinguisher, and the scrub technician threw pieces of ice toward the fire from across the room. The anesthesiologist disconnected a bag of intravenous fluid from the donor and used it to extinguish the fire.

The fire left a 10-by-5 inch area of sooting and singed skin on the right neck and shoulder where the breathing circuit had been. The donor's chin and face were reddened, and eyebrows, eyelashes and facial hair were singed. The patient was prepped again and the organ procurement was completed successfully.

Later, the surgeon speculated that had he started the fire by placing the electrocautery device next to the alcohol-soaked sponge wrapped around the tracheostomy.

Reference

1. Herman MA, Laudanski K, Berger J. Surgical fire during organ procurement. *The Internet Journal of Anesthesiology* 2009; 19: No. 1. ■

Splash and splatter risk often underestimated

The risk of infection from exposure to a patient's bodily fluids gained great attention over the past 20 years, spurred by the risk of exposure to HIV, and that heightened awareness has led to improvements in needlestick prevention. But another route of exposure to bodily fluids has not received adequate attention, say some experts.

Splashes and splatters can transmit disease effectively, but many institutions do not adequately protect against this risk, says **Susan Y. Parnell**, RN, MSN, MPH, CIC, director of employee health clinical services at the University of Texas Health Science Center in Houston.

"These exposures are grossly underreported," she says. "The risk of HIV and hepatitis B transmission through this route is lower than with a needlestick, but it is still a very significant risk."

Parnell advises risk managers to review their work practice control policies to determine if it adequately addresses splash and splatter risk by requiring protective equipment and protective measures when contact with blood and bodily fluids is "reasonably anticipated," as required by the federal Occupational Safety and Health Administration.

But what does "reasonably anticipated" mean? The work practice control policy should define those circumstances for your own organization, so that the frontline worker is not left to guess about each situation, Parnell says. The definitions will vary for each institution, based on variables

EXECUTIVE SUMMARY

The risk of infection from splash and splatter exposure often is not addressed adequately by health care providers. Staff must be educated about the risk and provided with proper protection.
- Expect some resistance from staff who do not understand the risk from splash and splatter.
- Risk managers may need to require the use of protective equipment, not just encourage it.
- Provide proper sizes of safety gear to encourage the best protection.

such as the type of patients treated, procedures performed, and patient volume. A trauma center may need to expect a splash and splatter risk with every patient, whereas a radiology department may not. Facilities treating the mentally ill and criminals may need to expect a higher likelihood of willful exposure through spitting, for instance.

"The next step is a product review. We're all pretty focused on sharps containers and related items, but we need to review the containers for body fluids also to make sure they have tight fitting lids to prevent spills and splash exposures," Parnell says. "Then you need to review your personal protective equipment. That is where you can gain the most ground in preventing exposures through splash and splatter."

Sizing of gear is crucial

Step one with personal protective equipment is to make sure it actually is available to clinicians. Parnell says the risk manager should ensure that all units have an adequate supply of the gear that can prevent bodily fluid exposure — protective glasses and goggles, face shields, hair covers, sleeve covers, long gowns, and gloves. And remember, it's not enough to just have a supply of these items. They have to fit the user, and that may mean keeping a variety of sizes.

"Many, many splashes occur because small nurses are wearing gloves that are too big for them, so they don't have a good grip. They lose control of a container or tubing and someone gets splashed," Parnell explains. "I used to see that a lot when I did acute care hospital employee health."

The work control policy also should specify what equipment is appropriate for different procedures and situations. Parnell says a risk manager, working closely with the employee health director, can have great influence in improving policies and procedures to prevent splash and splatter exposure. Get involved with the acquisition of protective equipment also, she suggests. Bring in the frontline employees, and let them review the products you're considering in a "product review fair." This can show employees that you are not simply buying the lowest bid products and that you want them to have the most effective supplies.

"A lot of what they say won't be new to you, but somebody's going to say something novel, point out a problem that you hadn't realized, or why one product is better than another for your facility. You really need to hear from those frontline nurses," she says. "We can't always buy the most expensive option, but if what they're saying ties directly to the injuries we're seeing in our data, the added cost can be justified, because injuries cost money."

Involving the staff also can reveal other issues that need to be addressed by the risk manager. For instance, Parnell says you may ask nurses to review protective equipment options, and one mentions that "My manager says we use too many of those, so she won't keep them on the unit." That's a managerial problem that must be addressed.

Staff may minimize risk

Educating staff about the risk from splash and splatter may be more challenging than talking about needlesticks, Parnell says. The risk from needlesticks has been ingrained in health care workers now, and people can more easily grasp how they could be infected by a needle actually puncturing the skin.

"Being splashed with some fluid is not as clearly an entry to the body, but bloodborne pathogens can cause infection if the circumstances are right," Parnell says. "It takes a little convincing sometimes to show people that this is a real health risk and not just a matter of avoiding something unpleasant on your face."

Splash and splatter exposures typically occur in the emergency department, the intensive care unit, and the operating room, says **Connie Steed**, MSN, RN, CIC, director of infection prevention at Greenville (SC) Hospital System University Medical Center in Greenville. Staff in those areas are at greater risk and should more routinely use the protective equipment that can prevent exposure.

"But we've seen splashes and splatters even in physician practices where they were doing a Pap smear or a cervical exam and didn't realize that there was a lot of secretions in that area," she says. "We've had people splattered in the eye with cervical secretions, believe it or not. That's not as common as some of the other scenarios, but these exposures can happen when people are not expecting it."

Steed says employees should be wearing facial protection any time they are performing high-risk procedures, such as intubations, suctioning with an open suction-type catheter, irrigating wounds with

SOURCES

For more information on splashes and splatters, contact:

- **Alicia Mares**, RN, CRNI, Clinical Marketing Manager, BD Medical — Medical Surgical Systems, Franklin Lakes, NJ. Telephone: (801) 565-2815. E-mail: alicia_mares@bd.com.
- **Susan Y. Parnell**, RN, MSN, MPH, CIC, Director of Employee Health Clinical Services, University of Texas Health Science Center, Houston. Telephone: (713) 500-3255. E-mail: susan.y.parnell@uth.tmc.edu.
- **Connie Steed**, MSN, RN, CIC, Director of Infection Prevention, Greenville (SC) Hospital System University Medical Center. Telephone:(864) 455-6267. E-mail: csteed@ghs.org.

a lot of drainage or secretions, or any procedure such as a bronchosopy that generates aerosols.

Facial protection is the key to reducing exposure, Steed says, but statistics for personal protective equipment usage consistently show that facial protection has the lowest rate of compliance.

"People just don't think splatter is going to happen, so they don't put on the protection. In our OR, we purchased eye protection that goes along with masks they wear, and now it is expected practice in our organization for them to use that eye protection all the time."

Bloodborne pathogen exposure to the eyes decreased to almost zero after Greenville Hospital System required the use of eye protection in the OR, she says. Making the use of such equipment mandatory is the most effective strategy, Steed says, but is only practical in the highest-risk areas. In other settings, providers usually must give the employee some leeway to decide when face shields or other equipment are needed, and unfortunately, they opt to forgo the protection too often.

Analyzing your exposure data can reveal which areas, procedures, and staff are most at risk of exposure from splash and splatter, pointing the risk manager in the right direction when making policy and urging better compliance.

"We saw that we were having a lot of exposure or potential for splattering in the ER during trauma care, so we educated them about that fact, and now we have made it routine for them to wear facial protection with those cases," Steed says. "Where you can make it routine, expected practice rather than leaving it to the individual to decide on a case-by-case basis, you'll always get better results." ■

Patients' mishandled funds could lead to RAC audits

Health care providers are becoming more familiar with the many errors that can trigger a RAC audit, but what is much lesser known among the health care community is that a patient's mismanagement of Medicare set-aside (MSA) funds post-settlement also could trigger an audit.

It is common practice that a MSA be created and approved by Medicare in workers' compensation, liability, or auto settlement cases that meet certain criteria. An MSA is a portion of a patient's settlement funds that are "set aside" as the primary source of paying for case-related medical expenses typically covered by Medicare, explains **Hany Abdelsayed**, a director with Rising Medical Solutions, a medical-financial solutions company in Chicago.

Misuse of those funds, however, can get a provider involved with a Recovery Audit Contractor (RAC). RAC represents the efforts of the Centers for Medicare & Medicaid Services (CMS) to recover overpayments to providers. The tendency is to assume that the patient is responsible for the appropriate use of those funds and, therefore, would be liable for any mishandling of the funds, but that is not necessarily the case, Abdelsayed says. When the MSA funds are misused, the government can come after the health provider.

"The government is getting much more aggressive in monitoring the payments they are making to medical providers, as well as the use of MSA funds," he says. "Through the RAC program, they are going out to search for money they paid in error and trying to recover those funds."

EXECUTIVE SUMMARY

A little-known risk for RAC audits involves how the patient handles a Medicare set-aside (MSA). Even though the health care provider is not in control of the funds, misuse of those funds could cause a big headache.

- Patients may be unaware or confused about proper use of MSA funds.
- The health care provider can be left holding the bag, even though it did no wrong.
- The admissions process should screen for this problem.

It is not enough for the health care provider to ensure it is doing everything right with Medicare billing, Abdelsayed says. Few providers realize they have to watch out for mistakes on the patients' part as well.

"Most often, the patient just doesn't know they should speak up about the primary payer, or they don't really understand how the MSA works," he explains. "If you tell them Medicare is paying for the treatment, that's good enough for them, and they don't complain."

Medicare wants its money

The problem arises when Medicare realizes it paid for treatment that should have been paid for with MSA funds or when a primary payer — an insurance company involved in the settlement — should have paid. If that situation is discovered, the provider could be subject to audit and would have to return the funds to Medicare, Abdelsayed explains.

"You have to give the money back, and then you have to start the collection process to try to get that money back from the truly responsible party — the patient or the primary payer," he says. "And you may have triggered a RAC audit that could uncover other problems."

The injured worker should be responsible for seeing that the proper source of funds was used for the treatment, but Medicare will go after the health care provider, because it has the money and they want it back, Abdelsayed says. It may not seem fair that the provider is the one that gets in trouble and suffers the financial loss, he says, but Medicare's primary goal is to recover the funds.

"Medicare may go after the injured worker, as well and jeopardize their Medicare benefits, but the provider is the real target," Abdelsayed says. "This could happen in a few months or a few years. By the time Medicare takes the money back, the provider is way behind in tracking down that patient and hoping he or she has some way to pay the bills."

To avoid this problem, health care providers should determine from the outset — even when the patient is eligible for Medicare and does not have private insurance — whether there will be a primary payer such as an insurance company, for the patient's treatment. Don't just assume that Medicare should pay for the treatment because the patient is eligible, or because other care has been paid by Medicare.

Any sort of injury on the job or suggesting a personal injury lawsuit should be a red flag for this hazard. The admissions process must include asking the right questions, because the patient may not volunteer that there is another source of payment.

"If someone comes in for treatment and indicates that there was some sort of injury involved, the medical provider needs to ask whether this will involve an insurance claim and any potential liability. If this is a slip-and-fall or any kind of workers' compensation claim, they need to identify who the primary payer will be, and that will be the insurance company involved in that claim," Abdelsayed explains. "Once they identify that, they need to ask if the claim has settled and if there is a Medicare set aside involved in this case." ■

SOURCE

For more information on RAC audits and MSA, contact:

- **Hany Abdelsayed**, Director, Rising Medical Solutions, Chicago. Telephone: (877) 747-4644. E-mail: hany.abdelsayed@risingms.com.

CME objectives

After reading this issue of *Healthcare Risk Management*, the CNE participant 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 health care for hospital personnel to use in overcoming the challenges they encounter in daily practice. ■

COMING IN FUTURE MONTHS

- ■ Avoiding psychiatric malpractice
- ■ Case study: A high-profile apology
- ■ Reducing liability risks in radiology
- ■ How to do effective background checks

CNE Questions

Nurses participate in this continuing education program by reading the issue, using the provided references for further research, and studying the questions at the end of the issue. Participants should select what they believe to be the correct answers, then refer to the list of correct answers to test their knowledge. To clarify confusion surrounding any questions answered incorrectly, please consult the source material. After completing this semester's activity with the **June** issue, you must complete the evaluation form provided and return it in the reply envelope provided in that issue in order to receive a certificate of completion. When your evaluation is received, a certificate will be mailed to you.

5. What is one provision of the HITECH act regarding enforcement of HIPAA?

A. It strengthened the civil money penalty scheme by establishing tiered ranges of increasing minimum penalty amounts, with a maximum penalty of $1.5 million for all violations of an identical provision.
B. It weakened the civil money penalty scheme by setting a maximum penalty of $50,000 for all violations of an identical provision.
C. It prohibited holding a health care provider accountable for any breaches by out of state attorneys general.
D. It established a 45-day time limit for authorities to propose penalties related to privacy breaches.

6. According to the results of a survey by HIMSS Analytics, what percentage of hospitals reported they would terminate their contracts with their business associates for violations of HIPAA?

A. 23%
B. 36%
C. 84%
D. 47%

7. According to Soham Roy, MD, which of the following is true regarding surgical fires?

A. Thoracic surgery is at the highest risk because gases can concentrate in pockets of the abdomen.
B. Head and neck procedures are at the highest risk of surgical fire due to the presence of exposed supplemental oxygen around flammable materials.
C. Brain surgery poses the greatest risk because it requires higher levels of oxygen.
D. Laparoscopic surgery poses the highest risk because flammable gases are contained within the closed body cavity.

8. According to Susan Y. Parnell, RN, MSN, MPH, CIC, what are the definitions for when splash and splatter exposures should be "reasonably anticipated?"

A. Any time a patient's wound is open or blood is exposed.
B. Only during surgery.
C. The definitions will vary for each institution based on variables such as the type of patients treated, procedures performed, and patient volume.
D. Only during trauma care.

Answers: 5. A; 6. D; 7. B; 8. C.

Healthcare Risk Management's
Legal Review & Commentary™
A Monthly Supplement

Suit alleges reaction to medication led to Stevens Johnson syndrome, death in elderly patient

By **Jon T. Gatto**, Esq.
Buchanan, Ingersoll & Rooney, PC
Tampa, FL

Lynn Rosenblatt, CRRN, LHRM
Risk Manager
HealthSouth Sea Pines Rehabilitation Hospital
Melbourne, FL

News: During a three- to four-month period, an 86-year-old man with a history of severe and varied health problems was transferred back and forth between a local hospital and nursing home for recurring urinary tract infections (UTIs). A few months later, the man was admitted to the hospital for recurrent urosepsis and scrotal cellulitis. A nurse noted the existence of a rash on that man's back and legs. The internal medicine physician ordered an infectious disease consultation for management of the UTI. The infectious disease physician ordered administration of imipenem and cilastatin, an antibiotic. A new rash appeared in response to the imipenem and cilastatin, and the physician ordered that the man take diphenhydramine. Seventeen days later, the man was taken to surgery, and vancomycin was added to the regimen in response to right scrotal drainage consistent with an abscess. A urology consult resulted in a recommendation to continue the IV antibiotic therapy and proceed with surgery of the left testicle. The imipenem and cilastatin and vancomycin continued after the surgery. After transfer back to the nursing home, the rashes on the man's body became worse. After seven days in the nursing home, the man was transferred back to the hospital, where he died. The man's estate settled with the hospital and nursing home for confidential amounts. The suit against two physicians resulted in a defense verdict.

Background: An 86-year-old nursing home resident had a medical history that included cerebral vascular accident, diabetes, arteriosclerotic heart disease, hydronephrosis, hypertension, and inability to swallow requiring placement of a gastronomy tube. The man was transferred between the hospital and nursing home during a three- to four-month span for recurrent UTIs. Soon thereafter, the man was readmitted to the hospital for recurrent urosepsis and scrotal cellulitis. A nurse assessed the man and noted the presence of a rash on his back and the backs of the man's legs. An internal medicine physician was the man's attending physician for six days and requested and obtained an infectious disease consultation for management and treatment of the UTI from an internal medicine and infectious disease physician. That infectious disease physician, after reviewing laboratory studies, ordered administration of imipenem and cilastatin in light of the fact that the infection may have involved *E. coli* and other dangerous organisms. The next day, the infectious disease physician was notified that a new rash had developed on the man's arms and upper chest. Acknowledging that the rash could have been caused by the imipenem and cilastatin, the physician treated the rash with diphenhydramine and did not discontinue use of imipenem and cilastatin. Seventeen days after hospitalization, the man was taken to surgery for treatment of the scrotal cellulitis on the left testicle. However, a week prior

to the surgery, vancomycin was added to the man's medication regimen to treat right scrotal drainage consistent with an abscess. The man's right testicle was removed during the surgery based on the existence of gangrenous scrotal tissue, despite the fact that the pathology report did not confirm existence of gangrenous tissue. The imipenem and cilastatin and vancomycin were continued after surgery.

A week after surgery, the vancomycin was discontinued, and steroids were administered. The physicians and nurses noticed an improvement in the rash, which had spread all over the man's body. The man was then transferred back to the nursing facility, where a skin assessment revealed dry, red rashes on his chest, back, and legs. Over the course of the next few days, additional blisters and rashes formed and were noticed by nursing home staff. After a week in the nursing home, the man was transferred back to the hospital and died 10 days later.

The man's estate settled with the hospital and nursing home prior to trial but brought suit against the attending physician and infectious disease physician, claiming that they had failed to adequately monitor and treat the man's scrotal cellulitis, which resulted in an abscess and the need for surgery. The claim also alleged that the physician failed to adequately monitor the complications associated with imipenem and cilastatin, which ultimately caused Stevens Johnson syndrome, a rare, serious disorder in which your skin and mucous membranes react severely to a medication or infection. All of these factors combined, alleged the plaintiff, contributed substantially to the man's death. A defense verdict was returned in the case against the physicians.

What this means to you: This patient is the classic nursing home resident with an extensive medical history and chronic ailments that are directly attributable to a long-term disease state and the physical deterioration that commonly accompanies advancing age. Significant in this cascade of deterioration is his pre-existing diagnosis of stroke, which most likely is directly accountable for his recurring UTIs. Stroke patients frequently experience neurogenic bladders that result in urinary retention. A man of this age also is likely to have benign prostatic hyperplasia or BPH, which also is a common cause of urinary retention. His hydronephrosis was directly attributable to urinary retention and a backup of urine into the ureters and kidney, all of which will cause UTIs.

Additionally, UTIs are treated with a multitude of different classes of antibiotics, dependent on the culture and sensitivity of the organism. Most urinary infections are bacterial in nature, and depending on the organism, will usually, at least initially, respond to common drug classes, of which penicillin and sulfonamides are most common. In cases where the patient has recurrent infections, treatment with more common antibiotics becomes less effective as the causative organism(s) become more resistant.

In this case, it is likely that the patient was actually colonized with multiple organisms. Colonization is a term used to describe the condition where the patient harbors the organism but does not actually demonstrate symptoms. In the case of urinary tract colonization, the organism can actually infect and reside in the bladder wall and, when the individual's immune system becomes threatened, the organism multiplies and the patient becomes symptomatic.

If the rash was of new onset, it could have been directly related to an offending organism or perhaps attributable to the antibiotics that had been used to treat the chronic urinary infections at the nursing home. Without knowing the medications he was on, it is impossible to attribute it to an interaction or acquired reaction.

What we do know is that the organism was most likely resistant, as imipenem and cilastatin are commonly used with multiantibiotic-resistant organisms. Since this was an institutionalized patient, it is not inconceivable that the physician was dealing with a super bug that is common with a chronically ill patient who had had multiple hospital admissions. We also knew that the patient did experience an outbreak of a new rash after starting the imipenem and cilastatin, and the physician did suspect that it may have been a reaction to the antibiotic. The physician treated it with diphenhydramine, but we are not told if it was effective.

Meanwhile, the patient experienced drainage from the right testicle and was started on vancomycin to treat right scrotal drainage consistent with an abscess. But a week later, he was taken to surgery for treatment of the scrotal cellulitis on the left testicle. The man's right testicle was removed during the surgery based on the existence of gangrenous scrotal tissue, despite the fact that the pathology report did not confirm existence of gangrenous tissue.

The antibiotics were continued after surgery, and the vancomycin was discontinued a week later. There is no mention that the patient had regular lab draws to determine the level of the

antibiotic circulating in the bloodstream following administration. Very high levels are an indication of impending toxicity with the potential for organ failure, particularly the kidneys.

Many of the patient's symptoms are classic to the patient's overall debilitated conditions from his dysphagia, for which he had a PEG, to his chronic kidney problems. The very fact that he had been on vancomycin could have predisposed him to liver inflammation. It can also be caused by herpes simplex or herpes zoster, which is the same virus associated with shingles, a common malady in the elderly, particularly when the autoimmune system is under stress. So, it is entirely possible that the nursing home and hospital staff attributed his overall decline to chronic disease and end-of-life decline. Besides, Stevens-Johnson is a rare phenomenon and generally treatable if the cause is determined and remedied before it becomes a systematic problem.

In this case, the physicians successfully defended their care to a jury. The hospital and nursing home settled most likely to avoid the cost of a jury trial. Had they not settled, it is entirely possible that they could have been exonerated, as well. Based on expert testimony, the jury most likely was unable to determine that treatment he received and the probable diagnosis of an allergic response to the antibiotics held greater weight than the man's overall chronic debilitation.

Given the outcome at trial, it may have been prudent for both the hospital and the nursing home to have collaborated with the attorneys representing the physicians in a unified defense, something that rarely happens. Generally, lawsuits involving both physicians and providers are seen as the enemy camps and this, as this case proves, can be counterproductive.

Reference

• Los Angeles County Superior Court, Case No. BC359018. ■

OB/GYN case results in $30M verdict

News: A pregnant woman sought prenatal care from a hospital-based OB/GYN practice. During the pregnancy, the woman had several ultrasounds that revealed some density in the fetal heart. However, no special plans were made for the child. At a regular office visit, her physician informed her that she might be a good candidate for vaginal birth after cesarean. The procedure was scheduled for three days later. After starting oxytocin, the woman experienced decreased variability. Ultimately, an emergency cesarean was required, and the baby was found outside the uterine cavity. A jury returned a verdict against the hospital and in favor of the plaintiff in the amount of $30,953,181.

Background: A third-time pregnant woman obtained prenatal care from a local OB/GYN. The woman's first two pregnancies and births had been uneventful, with the first as a vaginal delivery and the second as a cesarean.

The woman, based on the recommendation of her physician, had several ultrasounds. The ultrasounds revealed density in the fetal heart; but since the woman's caregivers determined that there was no interference in the fetal heart's function, no additional action was taken.

As the woman came closer to her due date, her physician determined that she may be a good candidate for VBAC, or vaginal birth after cesarean, based on the baby's position as head-down. The woman went into labor and presented at the hospital, where oxytocin was started to speed up the delivery process. The woman experienced decreased variability and was placed on oxygen and increased oxytocin. During labor, the fetal heart monitor showed a decrease in fetal heart rate, and the woman was taken to the operating room for an emergency cesarean. During labor, the woman's uterus ruptured, and the placenta was found completely detached with the baby outside the uterine cavity. Attorneys in the case alleged that the child probably went 18 to 20 minutes without oxygen.

The baby was born with APGAR scores of 3/4/4 at 1, 5, and 10 minutes, respectively. He remained at the hospital for 17 days until he was transferred to a specialty children's hospital and soon thereafter diagnosed with hypoxic ischemic encephalopathy, birth asphyxia respiratory depression and gastrointestinal hemorrhage. He was released from the hospital nine days later, but suffered from permanent and irreversible brain damage, cerebral palsy, and seizures, leaving him unable to speak or walk, and requiring 24-hour care.

On behalf of the child, the woman and her husband brought suit against the hospital, the OB/GYN physician, and the physician's practice group. The plaintiffs alleged that the hospital fell below the standard of care by failing to have in

place proper policies and procedures with regard to physician attendance and monitoring of at-risk patients, such as those that are considering VBAC and oxytocin. The complaint also alleged that the hospital nurses failed to tell the attending physician when the woman's contraction pattern became inappropriate, and that they continued to administer oxytocin despite the fragile nature of VBAC. The hospital presented the affirmative defenses of contributory negligence, assumption of risk, and failure to mitigate damages. The suit further alleged that the physician had failed to adequately manage the woman's labor.

A jury found in favor of the physician and his practice group but returned a verdict against the hospital in the amount of $30,953,181, the largest ever returned for a medical malpractice suit in Ohio.

What this means to you: Ninety percent of women who have undergone cesarean deliveries are candidates for vaginal birth after cesarean or VBAC, as it is frequently referred to. The greatest concern for women who have had a previous cesarean is the risk of a uterine rupture during a vaginal birth. According to the American College of Obstetricians and Gynecologists (ACOG), if the woman had a previous cesarean with a low transverse incision, the risk of uterine rupture in a vaginal delivery is 0.2% to 1.5%, which is approximately 1 in 500. Some studies have documented increased rates of uterine rupture in women who undergo labor induction or augmentation."

VBAC is done on a trial labor basis and only after careful discussion between the obstetrician and the patient. Essential is a low uterine transverse scar from a previous cesarean, no more than two previous cesareans, but at least one vaginal delivery, and no indication during the pregnancy that a cesarean would be necessary due to anatomical abnormalities of either the mother or the fetus. A VBAC should never be considered if the pregnancy poses significant risk beyond the fact that the mother had a cesarean previously. Another major consideration is that a physician is available to monitor the labor, and the hospital has the staff ready to do an emergency cesarean.

It would appear that this patient met the criteria, and one would assume that the obstetrician did speak with the patient and her husband and they were in agreement with the VBAC. The woman apparently experienced early signs of labor and went to the hospital. It is not known how long she had been in labor, but it appears that once she arrived, she was started on IV oxytocin to hasten her contractions.

Mothers who receive oxytocin during labor frequently report increased pain with contractions and frequently use pain medication to handle the increased pain, which can slow the infant's heart rate. Oxytocin requires an IV for administration and continuous monitoring to detect complications and/or determine the progress toward delivery. The drug can cause prolonged contractions and increases the possibility of a uterine rupture. There is an increased likelihood of a fetal malpresentation or malposition, and use of the drug is associated with an increased need for cesarean surgery for dystocia and fetal distress. Oxytocin is known to increase the likelihood of depressed fetal heart rate patterns and the chances of fetal distress due to decreased oxygen availability resulting in the need for urgent cesarean. For these reasons, the use of oxytocin is contraindicated for women desiring VBAC or, if it is used at all, it must be closely monitored and the obstetrician must be immediately available should any evidence of fetal distress or maternal complications, such as uterine rupture, occur, as these are life-threatening emergencies.

Another factor was that the infant had shown a possible issue with heart muscle density, which could have caused problems with oxygenation during labor if the fetus was stressed during prolonged contractions. The mother showed variability in the duration and strength of her contractions, and the oxytocin was increased. The big question is: Where was the obstetrician during the woman's labor and who ordered the increased oxytocin?

The infant was born with classic anoxic ischemic encephalopathy, which is brain damage due to oxygen starvation. The allegations brought in the suit certainly seem to fit the tragedy that ensued. This mother experienced the ultimate tragedy of a poorly managed labor resulting in a defective infant. In this case, the obstetrician was extremely lucky, as in many of these cases the jury finds against the physician as well. The amount of this judgment is excessively large, but OB cases are known for huge awards. While this case appears to be directly related to negligence, there are many similar cases where everything was done correctly, and the outcome was just as disastrous.

Reference

• Court of Common Pleas of Ohio, Montgomery County, Case No. 2006-CV-05798. ■

HIPAA Regulatory Alert

Supplement to *Healthcare Risk Management* and *Hospital Access Management*

HHS increases penalties for HIPAA violations

It's not just the organization at risk, but individual staff members

The U.S. Department of Health and Human Services has published an interim final rule incorporating provisions of the Health Information Technology for Clinical and Economic Health (HITECH) Act related to HIPAA violations that significantly increase the penalties it can levee against employers and health care providers.

Before the HITECH Act, businesses could incur a maximum fine of $100 for a single violation and $25,000 for all identical violations of the same provision. Now, however, there is a series of tiered minimum fines for individual claims and a $1.5 million maximum fine when a group of employees is affected.

HIPAA compliance executives and consultants have been quick to react to the new interim rule. "The new penalties are scary, and I think it really has all of us wanting to go back and review our HIPAA policies and procedures," says **Kathy Westhafer**, RHIA, CHPS, program manager, clinical information at Christiana Care in Wilmington, DE. "Even though we knew they were going to do this anyway, it has created real urgencies."

But **Cassi Birnbaum**, RHIA, CPHQ, director of health information at Rady Children's Hospital of San Diego, was much more sanguine. "Being from California, we have already had to be held to a much higher standard, so we really have a leg up," she explains. "In comparison to ours, it actually looks mild; we're not exactly shaking in our boots." However, she adds, "It can be very frightening if in the past you've just been held to minimal HIPAA penalties."

"I think the biggest issue is that a variety of things have come together," adds **Margret Amatayakul**, MBA, RHIA, CHPS, CPHIT, CPEHR, CPHIE, FHIMSS, who heads a Shaumburg, IL-based consulting firm that bears her name. "First of all, HITECH brings an enforcement rule that increases the size of the penalties; there's more at stake if there is an egregious violation. But there is a tiered approach that still enables a person who just didn't understand, or who tried hard to do what's right and still got in trouble, to be able to have a corrective action plan and perhaps lesser penalties than someone who does things with malicious intent. And this has been made clearer."

The new rule also makes clear, she continues, that it's not just the organization that is at risk, but if an individual member of the workforce does something wrong, they themselves can be held accountable. "You still have to train people, monitor them, and so on, and it's likely that if an individual gets in trouble, the organization will, too; but an individual who does something maliciously will see consequences — where in the past the organization would suffer the consequences directly from the government," Amatayakul says.

Three categories of violations

The interim rule spells out three different classes of violations:

"(A) In the case of a violation of such provision in which it is established that the person did not know (and by exercising reasonable diligence would not have known) that such person violated such provision, a penalty for each such violation of an amount that is at least the amount described in paragraph (3)(A) but not to exceed the amount described in paragraph (3)(D);

"(B) in the case of a violation of such provision in which it is established that the violation was

due to reasonable cause and not to willful neglect, a penalty for each such violation of an amount that is at least the amount described in paragraph (3)(B) but not to exceed the amount described in paragraph (3)(D);

"(C) in the case of a violation of such provision in which it is established that the violation was due to willful neglect — (i) if the violation is corrected as described in subsection (b)(3)(A),\1\ a penalty in an amount that is at least the amount described in paragraph (3)(C) but not to exceed the amount described in paragraph (3)(D)."

While the minimum penalty varies with each category, the maximum is the same in all cases: $1.5 million. With such significant dollar amounts at stake, it's critical to understand exactly what is meant by each of these types of violations.

For "Category A," Amatayakul offers this hypothetical: "Let's say the breach was from a paper-based record — somebody looked at it or overheard something or saw somebody [famous] in the hospital. They did not have malicious intent, but somehow there was a breach."

There is no way to absolutely say you can monitor everybody who works on a paper-based record, she continues. "Obviously, training needs to be done, and the government will be looking at the extent to which you did train people, gave them examples of this type of breach, told them it was wrong, and secured the information in such a manner as to make it more difficult to casually see something you shouldn't," Amatayakul shares. "Even in an electronic environment there could be a person who has legitimate access to the information — maybe a nurse who takes care of the patient — but they happened to tell somebody something they shouldn't have."

A "Category B" violation, Amatayakul continues, "might be where a VIP is in-house and a person comes to learn of their alias or snoops. There is no malicious intent, like selling a story to the *National Enquirer;* they are just curious, but they know they shouldn't be doing this, so the penalty would be stiffer."

For the most serious type of violation, "Category C," the onus falls much more heavily on the organization.

"This would be more a case of an organization not having very strong access controls," suggests Amatayakul. "They did HIPAA training the first time it was enacted, but never did any more training. Or, they have a policy on sanctions but they don't do anything about it."

The interim rule does provide for a time period in which corrective action can be taken, and such actions can reduce the penalties.

Your corrective action plan, says Westhafer, "is really part of reviewing your policies and procedures and setting things up so you know what the remediation plan is up front. I almost think of it like disaster planning — you think about what things can go wrong, and as you go through your policies and procedures, and what the protocol is going to be for each type of violation, so you're a step ahead."

Hospitals, she continues, should be used to this type of preparation. "We get surveyed all the time from The Joint Commission and others, so we know if a situation arises, we're pretty used to jumping in and we know we have to take care of it quickly," Westhafer notes.

"We have developed a grid," says Birnbaum. "We wanted to make sure to have community-wide standards so we did it in conjunction with other privacy officers in San Diego, and in fact just updated it to clarify the reporting process and responsibilities." Under the policy, for example, for a first-time inadvertent breach, verbal counseling is given; if there is a subsequent trend, it will result in a final written warning.

"The big thing for us is the need to consistently apply the policy to all members of the workforce," says Birnbaum. "You can't be more lenient with 'Suzie Q' just because you like her."

She adds that even though she provides education at the time of new employee orientation, "We now have an additional course that is a new requirement for every work force member — including medical staff. Also, we've passed around the policy so people will know the repercussions of violations."

"It's more likely than not the OCR [The Office for Civil Rights, which handles HIPAA enforcement] will look a little more carefully at whether the corrective action plan is appropriate, and they may move to a civil monetary penalty if they feel it is not strong enough or it is not the only thing that should have been done," offers Amatayakul. "In the past, they just sort of assumed everybody would do a corrective action plan and gave everybody an opportunity. They were nice, and helped you overcome the issue."

Now, she says, "They're under the gun to be a

little bit tougher. Not only is the OCR under the gun to be more proactive, but there is an incentive for them to give out civil money penalties because they get to keep some of the money; they can also turn some of it over to the individual who is harmed."

In the past, she says, the OCR didn't have the staff to go after violators as aggressively. "They were cranking out these letters, asking facilities to come up with a plan," she recalls. "Now, with a little bit more money, and now with [HIPAA] security under OCR (in addition to privacy) they are likely to be a positive force. They want you to do the right thing, and it makes them feel better if they help the [harmed] individual."

In terms of how they will view corrective action plans, she adds, "They will look for more specific evidence that this was done, and that action was taken." Whether you have acted on your plan, she stresses, has now become more important. "People in that situation [of being found in violation] need to come up not just with a specific plan, but with evidence they put it into action," Amatayakul warns.

[For more information, contact:
***Margret Amatayakul**, MBA, RHIA, CHPS, CPHIT, CPEHR, CPHIE, FHIMSS, Margret\A Consulting, LLC, Phone: (847) 895-3386. E-mail: Margret@Margret-A.com;*
***Cassi Birnbaum**, RHIA, CPHQ, Director of Health Information, Rady Children's Hospital of San Diego, CA. Phone: (858) 966-4095. E-mail: cbirnbaum@rchsd.org;*
***Kathy Westhafer**, RHIA, CHPS, Program Manager, Clinical Information, Christiana Care. Phone: (302) 327-3815, E-mail: kwesthafer@christianacare.org.]* ■

Sharing user names is a HIPAA security violation

What's a shared user name between friends? Quite a bit, when it comes to the HIPAA security rule, warns **Marion Jenkins**, PhD, co-founder of QSE Technologies Inc., an Englewood, CO-based technology consulting firm. Unfortunately, he adds, many organizations have individuals who share user names — some because they are unaware of the seriousness of the violation, and others because they have less honorable intentions.

"Generally, the initiative comes from the health care workers — although sometimes it is initiated by management," says Jenkins. "It could simply be out of convenience; people become frustrated with all the different passwords they have to use so they either decide to use common ones, write them down, or share them."

Let's say there are part-time employees who only come in once a month and are replaced from time to time. "What often happens is that you give everyone access because it's a pain to change user names on and off," Jenkins explains. "So during implementation, you may make everybody a super-user. But that's a total violation of HIPAA."

Health care organizations that allow shared user names to avoid additional licensing costs are opening themselves up to a "double-whammy" of HIPAA violation penalties *and* hefty fines for violating licensing agreements. "You may have a software package that charges $1,000 for a login, and that software may be used by a number of part-time people," Jenkins posits. "Many vendors will give you device licenses vs. user licenses, which allow you to have one person on at a time per machine, and that's the way you should do it. Some vendors, however, do not do this, so management seeks to circumvent licensing fees [by sharing user names]."

Microsoft Office, he notes, retails for about $300-$400. "If you are found violating that software agreement, you can be fined $3,000 per instance; so if you have 20 workstations and can't produce 20 licenses, you're looking at a $60,000 fine [in addition to HIPAA violation penalties]," warns Jenkins.

Defeating intent of security rule

The key issue, Jenkins continues, is that such a practice completely defeats the intent of the HIPAA security rule. "HIPAA security requires that with anyone who accesses or changes or looks at [protected health information] you have to be able to tell who did it and when," he explains. "If you have a user logged in at a nurse's station on a given day, and you do not know who it was among the eight rotating nurses, it's a violation. It says very explicitly in the security rule that with anyone who can access, view, edit, or change an entry you have to be able to tell who did it and when. There has to

be an audit trail."

In addition, says Jenkins, "it defeats the most basic security policies that represent industry best practices. It makes it difficult to troubleshoot many IT problems, and it can jeopardize your human resource operations if you forget to change user names if and when an employee leaves the company."

So, what should your policy be with regard to allowing employees to share user names? "If you are tempted to share login names, don't," Jenkins warns. "If you are currently doing it, stop. Get yourself in compliance with the HIPAA security rule by having each employee — whether part-time or full-time — use a unique user login name."

Part of the problem, Jenkins suggests, stems from the fact that there are two distinct HIPAA rules — one governing privacy, the other governing security. "HIPAA security is completely different, and many facilities do not understand it," he asserts. "So many of them had been so 'beaten up' by the privacy rule that when the security rule came along, they went to sleep."

Your organization is required to have a completely separate set of procedures around HIPAA security in addition to those around privacy, Jenkins continues. "For example, you need to have a HIPAA security officer; it may be the same person as your privacy officer, but it *has to be formalized*. You have to physically secure your computer equipment. You must maintain a log of all security incidents — so, for example, in the case of a hard drive or power supply failure, you must record who entered the room and what they did."

Specifically around user names, he adds, you must have different ones for every individual. "In addition, that user name and password should only allow them to access what they need; so, for example, billing people should not be allowed to see clinical notes," he explains. "Furthermore, there must be different levels of security; for example, some employees will be allowed to view certain information but not to change it." The most important thing of all, he concludes, is to make sure you have delineated a clear distinction between HIPAA privacy and HIPAA security. "Satisfying one does not satisfy the other," he cautions.

[For more information, contact:

***Marion K. Jenkins**, PhD, QSE Technologies, 359 Inverness Drive South, Suite K, Englewood, CO 80112. Phone: (303) 283-8400, ext. 115. Fax: (303) 283-8401. E-mail: Marion.Jenkins@qsetech.com.]* ■

HIPAA requirements, penalties increased

According to the Ambulatory Surgery Center Association, the economic stimulus package passed by Congress last year included several changes to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) involving privacy of patient information:

- The penalty for violations increased from $100 per penalty to $1,000 per penalty. The maximum penalty is $100,000. If the violation involves willful neglect, the violation per penalty is $100 to $1,000, and the maximum penalty is $100,000.
- When an unauthorized disclosure occurs, facilities have a greater obligation to alert patients and the government. Unless the information was "secured," facilities will be required to notify those whose protected health information was involved. The Centers for Medicare & Medicaid Services (CMS) issued guidance last spring that said information must be encrypted or destroyed to be considered "secured." In some circumstances, facilities must notify the federal government and the media about the unauthorized disclosure.

Patients can prevent providers from giving information to payers about services for which the patient pays directly. This change will require modification of some contracts, the ASC association points out.

Facilities that use electronic medical records (EMR) will be required to provide patients, upon request, with a list of all disclosures made through the use of an EMR for the prior three years. The implementation date for this provision depends on when the Department of Health and Human Services issues rules, but the earliest implementation date will be Jan. 1, 2011. Most of the other changes go into effect in 2010; however, increased penalties for violations have been in effect since Feb. 17, 2009.

On Feb. 17, 2010, facilities using EMRs will be required to provide individuals a copy of their record electronically, upon request. Facilities can charge for the labor costs. ■