Healthcare Risk Management™

October 2010: Vol. 32, No. 10
Pages 109-120

IN THIS ISSUE

Financial Disclosure: Author Greg Freeman, Managing Editor Karen Young, Executive Editor 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.

Facebook, other social sites continue posing risk problems

Nurse fired after commenting online about treating "cop killer"

Social networking sites such as Facebook and MySpace continue to be a tricky problem for health care risk managers, who need to ensure that employees do not violate patient privacy even when off duty — but also must avoid violating the personal rights of those employees. Failing to address the situation adequately could mean a HIPAA violation or damage to the provider's reputation, but using too heavy a hand could run afoul of labor laws.

Facebook and other sites have been a difficult issue in health care for as long as the sites have been around, but the growing popularity brings added concerns, says **Sharona Hoffman**, JD, professor of law and bioethics and co-director of the Law-Medicine Center at Case Western Reserve University School of Law in Cleveland. Not only are more people using the sites, but people are becoming more complacent about posting information on them, often giving little consideration to the fact that a post on a social networking site can be viewed by a large number of people, if not everyone, and the information can be copied and posted elsewhere, Hoffman says. This problem of complacency, thinking nothing of posting innermost thoughts or work-related rants, can be most prevalent among younger people who grew up using social networking sites, Hoffman says.

"Everyone else gets to [go] home and vent about their boss or the work they had to do that day, but health care providers sometimes don't under-

EXECUTIVE SUMMARY

Employees run the risk of violating HIPAA when posting information about their work on Facebook or other sites. Hospital policies must address this ongoing risk without violating employee rights.

- Patients can be identified even if the employee does not post a name.
- Employees can become complacent about posting online.
- Providers should not try to forbid all posting by employees.

AHC Media LLC

stand that their situation is different," Hoffman says. "People have [been] disciplined for posting patient information, pictures, and videos of surgery. There have been cases where people posted pictures of themselves, but a patient chart was in view. That's problematic."

The ongoing problem was illustrated recently by a case in Detroit, when Cheryl James was fired from her job as a nurse at Oakwood Hospital, after posting a statement on her Facebook account indicating her displeasure with having treated a "cop killer" that day, according to a statement released by the hospital. (*See the story on page 112 for more details.*)

The posting did not include the patient's name, but Hoffman says this is a good example of how employee education sometimes fails. The nurse may have sincerely thought that she was not violating HIPAA because she did not identify the patient, Hoffman explains; but the patient was identifiable because there was ongoing media coverage about the shooting incident. And it was well known who the alleged "cop killer" was. Employees must be educated about how they can violate HIPAA, even without publishing names.

"The incident also shows another problem with these postings, and that is the way an employee's social networking comments can damage the hospital's reputation," Hoffman says. "Nurses and doctors are supposed to just care for their patients and not think about who they are or what they've done, so a public comment like this can be very damaging to the hospital. A hospital is certainly within its rights to take disciplinary action against an employee who says treating certain kinds of patients is distasteful."

James will fight her termination, because she says she did not violate HIPAA, and the hospital violated labor laws by dismissing her, according to a story on MyFoxDetroit.com (http://www.myfoxdetroit.com/dpp/news/local/oakwood-hospital-employee-fired-for-facebook-posting-20100730-wpms). Healthcare Risk Management made several calls to James' attorney seeking comment, but they were not returned. She isn't likely to prevail, says **David Gevertz**, JD, a shareholder and vice chair of the labor and employment department at the law firm of Baker, Donelson, Bearman, Caldwell & Berkowitz in Atlanta. The hospital will be able to show that the posting violated HIPAA and — most likely — that it violated the hospital's own policies about what information can be shared regarding patients, he says.

The hospital's policy can be the linchpin in such cases, Gevertz says, but he also cautions that it can be a mistake to go too far with prohibitions on what employees can post online. The provider must insist that website postings not violate HIPAA or any other law for which the health care organization is accountable, but stating that employees may not post about their work or the

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.
Managing Editor: Karen Young (404) 262-5423 (karen.young@ahcmedia.com).
Executive Editor: Russ Underwood (404) 262-5521 (russ.underwood@ahcmedia.com).
Production Editor: Neill L. Kimball.

Editorial Questions

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

provider is going too far, he says. (*See page 112 for more on social networking policies.*)

"I do not advise that health care providers adopt blanket prohibitions on the use of social media. Such prohibitions limit the creation of innovative ways to use new technologies, hamstring employers into making unfortunate personnel decisions, and expose employers to liability for invasion of privacy," he says. "Instead, I counsel that the best approach is to develop a task force within the client's company that includes employees from the human resources, marketing, information technology, compliance, legal, and risk management departments. That group should then explore the utility of social media to their organization's culture in order to develop a clear scope of the activities it wishes to regulate."

One attorney cautions risk managers not to think of website postings as unique from other forms of communication. No matter how the information is disseminated, the same basic rules apply, says **Kevin Troutman**, JD, an attorney with the law firm of Fisher and Phillips in Houston.

"This comes up regularly, and we generally advise clients to consider their existing policies and update them to reflect the existence of Facebook and similar sites," he says. "In essence, they should treat an employee's statements on a public website the same way they would treat those statements if made orally in another public or semi-public forum. Patient privacy policies still apply, as do policies regarding other confidential information or public comments about the hospital."

On the other hand, hospitals have to be careful not to violate employee privacy rights and/or their rights under the National Labor Relations Act, says **Leslie Spasser**, JD, a shareholder with LeClairRyan in Virginia Beach, VA. Having a specific policy on social networking sites, with a signed acknowledgment from the employee, is an important first step in protecting the employer from charges that it ran roughshod over the employee's rights, she says. The information provided to the employee should make clear what is acceptable and what is not, and it should notify the employee of the possible disciplinary actions for violating the policy, she says.

"At the same time, it's critical to do training for the employees. HIPAA itself requires training, and I think you would benefit greatly from adding a Q&A session to discuss how the social networking policies apply," she says. "It forces employees to think about what is acceptable and what is not."

Employers have considerable leeway in disciplining and dismissing employees, but Spasser says it is always best to have clear policies in place and to provide notice to employees. That will greatly diminish the challenges from employees and provide a firmer footing if you are sued. Public employers may have more difficulty in this area, notes **Mark Nelson**, JD, an attorney with Drinker Biddle in Chicago. Public employers must consider state and federal constitutional protection of free speech rights, which can constrain them more than private employers, he says. Even so, private employers may have to consider state laws.

"For example, some states have laws that restrict an employer's ability to discipline or hold against an employee a lawful off-duty conduct in which the employee engages," he says. "Most of those laws concern activities like smoking, saying an employer can prohibit smoking in the workplace but can't ban employees from smoking when off duty. Depending on the wording of these laws, however, they could be applied to something like posts on a social networking site, particularly if it doesn't rise to the level of a HIPAA violation."

That is not to say that employers can't be firm. Hoffman says there is no problem in telling employees that they may not post information regarding patients.

"I think it is appropriate for an employer in the health care arena to say you do not post anything about patients in any way on your website," she says. "It's just too sensitive. Sometimes, you think it is not identifiable, but it is. Health care is not like being a car salesman. There is a higher level of responsibility, and it is appropriate to tell employees they cannot post anything about patients on their own websites and social networking sites."

However, the employer should not demand access to employees' website postings, she says. Spasser agrees, saying the courts are inconsistent now regarding how much employers can monitor employees' Internet postings and hold them accountable. It is better to educate employees about the risks than to depend on looking over their shoulders and checking what they post, say Spasser and Hoffman.

"Then, you get into some problems with employee privacy," Hoffman says. "Employees put all sorts of private information on their sites that is not meant for employers to look at. You have to balance the employee's rights and the patient privacy rights."

SOURCES

• **Sharona Hoffman**, JD, Professor of Law & Bioethics, Co-Director of the Law-Medicine Center, Case Western Reserve University School of Law, Cleveland, OH. Telephone: (216) 368-3860. E-mail: sxh90@case.edu.

• **Leslie Spasser**, JD, Shareholder, LeClairRyan, Virginia Beach, VA. Telephone: (757) 217-4535. E-mail: leslie.spasser@leclairryan.com.
• **Mark Nelson**, JD, Drinker Biddle, Chicago. Telephone: (312) 569-1326. E-mail: mark.nelson@dbr.com.
• **David Gevertz**, JD, Shareholder and Vice-Chair of the Labor and Employment Department, Baker, Donelson, Bearman, Caldwell & Berkowitz, Atlanta. Telephone: (404) 221-6512. E-mail: dgevertz@bakerdonelson.com.
• **Kevin Troutman**, JD, Partner, Fisher & Phillips, Houston, TX. Telephone: (713) 292-0150. E-mail: ktroutman@laborlawyers.com. ■

Nurse fired for off-duty post on Facebook

Nurse Cheryl James didn't think she was violating any rules when she posted her frustrations on Facebook, saying she had treated a "cop killer" that day.

The posting followed the shooting death of Taylor Police Corporal Matthew Edwards in July 2010. James was one of the nurses who helped treat the accused shooter, Tyress Mathews, at Oakland Hospital in Detroit after the incident.

James told Fox News that she was emotional after the events of the day, knowing that a police officer was dead and she had worked to save the life of the man accused of shooting him. After work one night, while at home, she vented her frustrations and anger on Facebook, saying she had come face-to-face with a "cop killer" and that she hoped he rotted in hell, along with other obscene comments, she told Fox News. (For the full story from the news site, go to http://www.myfoxdetroit.com/dpp/news/local/oakwood-hospital-employee-fired-for-facebook-posting-20100730-wpms.)

A few days later the hospital fired James, saying she had violated HIPAA by posting protected health information on Facebook and had made disparaging remarks about a patient. After the firing, Oakwood Hospital released this statement:

"As health care providers, we have a legal and ethical responsibility to protect patient privacy, and we are bound by HIPAA rules and regulations to ensure that we do so. All of our employees are trained and expected to protect patient information. This means keeping details confidential that might make it easy to identify a patient, even if his or her name has not been revealed. That's why disciplinary action, even termination, may result from sharing information about patients inappropriately in any public forum or setting. While we cannot discuss specific details regarding any current or former employee, we all have a legal and ethical responsibility to put our personal opinions aside and provide the care required for any patient who has entrusted us with their health." ■

Policy crucial to avoiding web breaches

Only about a quarter of employers have a policy on employees' use of social networking sites, says **Danielle Urban**, JD, an attorney with the law firm of Fisher & Phillips in Denver.

"Without a policy, it's harder to discipline and to fire an employee," Urban says. "We recommend that employers have policies against employees blogging, posting, or Tweeting anything that identifies that person as an employee of the organization. Or if you don't go that far, you can require employees to post a disclaimer that anything they say is not endorsed by the hospital and is being said only as a private person, not your representative."

Urban also suggests the policy include a requirement that the employee not mention a coworker, patient, vendor, or any other contact from work without obtaining permission from that person first.

"Remind employees that what they do on their private time can be a violation of company policy and maybe even the law," Urban says. "It's amazing how many people think they can post something on the Internet and it will be seen only by the people they want to see it. It's out there for people to see, and employers will find out about it even without doing anything sneaky to monitor what you do. These things can cost you your job."

Employers have a legitimate interest in limiting what their employees post, says **Amanda Vega**, a consultant in New York City specializing in social networking sites and media management.

"The written policy on the use of social networks should be signed by all employees, so there is no misunderstanding. The hospitals cannot say that employees are not allowed to use social networks, but they can have a policy clearly stating that they may not write, chat, take pictures, Tweet, or post on Facebook, etc., about any patient," Vega says. "This can also apply to stating information about any personnel within the hospital — doctors, nurses, interns, technicians, or medical reps."

Even after the written policy is in place, there should be at least an annual policy review and training for the employees in case there are any issues to address or new social networks that have come into play, she says.

"If the employee agrees to not post any patient information and does it anyway — this would include referencing a patient as a cop killer — this can be terms for a serious violation and/or termination," Vega says.

The best policies tend to limit Internet usage and prohibit most blogging or posting on sites while at work, says **David Gevertz**, JD, a shareholder and vice-chair of the labor and employment department at the law firm of Baker, Donelson, Bearman, Caldwell & Berkowitz in Atlanta. Gevertz says the policy also should include these points:

- Emphasize that employees remain responsible for the content of texting and Internet postings done outside of work.
- Reserve the health care organization's right to demand that the employee remove the information from the posting site.
- Strictly prohibit the dissemination of, posting, or reference to patient identifiable financial or health information.
- Reserve the company's right to monitor, review, and inspect all e-media use conducted through its networks and the contents thereof.
- Mandatory training on the policy should include examples of what is and is not appropriate material for public dissemination.

SOURCES

- **Danielle Urban**, JD, Fisher & Phillips, Denver, CO. Telephone: (303) 218-3650. E-mail: Durban@laborlawyers.com.
- **Amanda Vega**, New York City. Telephone: (646) 450-8342. E-mail: Amanda@amandavega.com. ■

Use data to prove value of RM to top brass

Risk managers have always struggled to prove the value of their work to health care administrators, because much of what they do consists of preventing expenditures and minimizing costs. A concerted effort to prove the worth of your department can result in a higher profile for risk management within the organization, greater stature for the risk manager, and improved resources.

Showing what you contribute is crucial for both your individual success and the future of risk management as a whole, says risk manager **Roberta Carroll**, ARM, CPCU, MBA, senior vice president with Aon Solutions, the risk management consulting company based in Chicago.

"After almost 40 years in risk management, I see that we need to make some dramatic changes in not only what we do but how we do it, or we're going to be a dying breed," Carroll says. "With the emphasis on patient safety officers, some CEOs could say, 'I have a patient safety officer who is managing the clinical aspects of risk management, and I have in-house general counsel for the claims, and my CFO can do the risk financing, so what do I need you for?'"

Risk managers must be able to carve out their own place in the organization, a significant role, and prove their value, Carroll says. There is a role that is going unfilled in most health care organizations, she says. There is no one who connects all the dots, looking at not just the surface problems such as malpractice claims, for instance, but deeper into the many causes of the mistake that led to that claim. Risk managers are ideally suited for that role and should start moving themselves into that kind of key leadership position, Carroll says.

The big picture is the future of risk management, she says. For instance, many providers have a fleet of vehicles to manage. Who is looking at fleet safety? When Carroll worked in a health system, it had 120 cars and more than 300 drivers. That was a significant risk for her, and she addressed it with safe driving programs, a claims reporting process, and other preventive measures. Then she measured the results before and after. That is the kind of wide-ranging risk management that she recommends as a way to improve your value to the organization.

"Risk managers are at the cusp of either some-

EXECUTIVE SUMMARY

The best way to prove the value of your risk management efforts is by presenting hard data to top executives. Focus on the quantifiable savings from improved patient safety and lower workers' compensation costs.

- Provide proof of the department's value on a regular basis.
- Present the information in the way upper management likes to receive data.
- Consider risk management a profit center rather than an expense.

thing wonderful or potentially their demise," she says. "I see some real possibilities if they take the opportunity that's in front of them now."

Have to blow your own horn

Just saying you are doing a good job, or hoping that upper management notices, is never enough. Risk managers should present data that prove the department's success, says **Cindy Berry**, chief health care strategist with SAS, a software and analytics company based in Cary, NC. That isn't always easy to do, however, because risk managers often compile data in the way that best suits their needs and not in a way that will present well to upper management, she says.

"Most of the systems risk managers use are not really great for reporting to senior management," she says. "A lot of times, we see a lot of manual work being done to report to upper management, and they can't really see the magnitude of the work risk managers do. They also can't see trends or efforts for improving that process."

Better data management and the use of analytics can yield more persuasive information, but Berry cautions that you can't just focus on your own in-house data. You also should be presenting data from outside your organization as a comparison. Carroll says risk managers traditionally have not been very good at quantifying the effects of programs they implement, particularly when it comes to anticipating and then documenting the actual change in their own organization, as opposed to goals and hopes.

Berry agrees that data is king.

"You might be doing a phenomenal job, but if [you] have no data to show what the rest of the health care world is doing, nobody can really tell how well you're doing. With that data, then you can show that you had 12 hospital-acquired infections last year, and after our risk management initiative this year, we only had two," she says. "The rest of the industry averages 20, and we can look at this financial data to see that every additional infection costs us an additional $60,000. So, we saved our organization $600,000 over last year and $1,080,000 compared to other hospitals."

This type of information often is presented through quality committees, at the board level, Berry says. Participating in quality committees creates good exposure at a high level within the organization, she says.

"If your committee meets monthly, that is ideal, because you can present this data each month and see the trends going up or down," she says.

Keep information flowing

This type of information should be presented regularly, on an ongoing basis, she says. Don't think that you can't schedule a meeting with executives once or twice a year and do a big presentation to justify your department, she says. Berry notes that risk managers should not be dissuaded from presenting risk management data because they do not have all the data they want — or because it is not in the most useful form. Anything is better than nothing, she says.

"If you don't have access to integrated data that paints a full picture, start with critical event reports on some of those measures that Medicare is going to start cutting payment for, like hospital-acquired infections," she says. "Work with your quality department to get data on issues like that, and start building your presentation. Then, you can track three or four core quality measures that you're already tracking for the government anyway."

Then you should work with someone in the organization who can help tie that information into financial data, Berry says. Remember that in the C-suite, they will want to know the dollar impact, not just that you did a good thing by improving quality or safety.

"Find someone who can tell you that for every hospital-acquired infection you avoid, this is how much money you're saving, because the government doesn't pay for them anymore," she says.

Workers' comp ripe for analysis

Some areas of risk management lend themselves better to statistical analysis than others, says **Timothy Folk**, a partner with the Health & Human Services Industry Team at The Graham Company, a risk management consulting firm in Philadelphia. Workers' compensation claims are one of the best options, because their high frequency and high severity lead to more statistically relevant data, he says.

"With other types of claims, like professional, property, or general liability, you may only get one claim every couple of years, or even if you get a few more, you're still not able to gather the volume of data necessary to make it statistically relevant," he says.

With workers' compensation claims, Folk says the data can be compiled over several years and then broken down by many factors, including the details of how the injury happened, the time before

settlement, and medical vs. indemnity ratios. That breakdown can point to trends in your workers' comp claims and then relate those to the training provided to employees and the results of your risk management efforts.

"You can show to upper management the changes in lost days, settlement costs, all the associated costs that come with a workers' comp claim," Folk says. "Workers' comp is probably the most data-heavy opportunities you have [to] present your work to management, even if it isn't as exciting as some other risk management activities."

Reserves are critical subject

Be sure to focus on reserves when discussing worker's compensation with upper management, says **Christopher Keith**, also a partner with the Health & Human Services Industry Team at The Graham Company in Philadelphia. Executives will be most interested in reserves in relation to workers' compensation management, because that equals cash flow, he says.

"You want to really aggressively manage those reserves and show how you are managing the claims to closure," he says. "Another way to drive up your reserves is with the medical to indemnity ratio. A good rule of thumb is that you should have an 80/20 ratio, meaning 80% should be medical-only and 20% should include indemnity loss."

Keith recalls working with a client that had a 60/40 ratio, meaning 40% of the workers' compensation claims involved lost time. The indemnity claims were costing an average of $21,000 per claim, but the medical-only claims were costing an average of $5,000. Reducing those indemnity-related losses with light-duty programs and other strategies can significantly improve the ratio, which can be demonstrated to management.

Folk points out that it also is important to adjust your costs and exposures over time when discussing long-term trends in claims management or other risk activities. Particularly in a down economy, the data can be misleading if you do not account for changes in your exposures. If your organization has downsized and has fewer employees, for instance, the exposure to certain risks may have decreased.

"You don't want to give upper management a false read on the performance of risk management," Folk says. "If your premiums have gone down, and you don't adjust for contracted or expanded operations, it makes the statistical balance irrelevant."

SOURCES

- **Cindy Berry**, Chief Healthcare Strategist, SAS, Cary, NC. Telephone: (919) 677-4444.
- **Roberta Carroll**, ARM, CPCU, MBA, Senior Vice President, Aon Solutions, Chicago. Telephone: (312) 381-1000.
- **Timothy Folk**, Partner, Health & Human Services Industry Team, The Graham Company, Philadelphia, PA. Telephone: (215) 701-5231. E-mail: tfolk@grahamco.com.
- **Christopher Keith**, Partner, Health & Human Services Industry Team, The Graham Company, Philadelphia, PA. Telephone: (215) 701-5297. E-mail: ckeith@grahamco.com. ■

Think of RM as a profit center, not an expense

Here's a radical idea: Instead of trying to show management why your department is worthy of respect, go on the offensive and declare that risk management is a profit center every bit as much as that shiny new cardiac center or the plastic surgery clinic.

That approach makes sense when you look at the current activities of a risk management department, says **Edwin Foulke Jr.**, JD, former assistant secretary of the federal Occupational Safety and Health Administration (OSHA) and now co-chair of the Workplace Safety & Catastrophe Management Practice Group with the law firm of Fisher & Phillips in Atlanta. Over the years, most businesses have focused on efficiency and quality, with strategies such as Six Sigma and Continuous Quality Improvement, and as a result they have become more profitable, Foulke says. Health care providers have been following the same path as other businesses, and they are finding that they have exhausted the obvious ways for improving revenue.

"Companies have been able to achieve a lot of cost savings and become more profitable and more competitive, but as you squeeze anything you get to a point where it becomes harder to achieve any more cost savings," Foulke says. "So, the question becomes what areas are left where they can achieve cost savings; there are really only two areas left — workers' comp and health care. And risk management is what deals with those two areas."

Risk management traditionally has been seen as an expense on the liability side of the ledger and not as a potential profit center, he says. That is partly because business schools and MBA programs rarely include instruction on occupational safety and health, much less how risk management and safety can improve profit, he says.

Show how you make money

The savings from risk management must be quantified and presented as not just money you didn't lose, but rather money that contributed to the bottom-line success of the organization. In other words, Foulke says, show that risk management actively makes money for the organization, rather than just helping avoid losses.

Risk management's efforts to improve workplace safety by reducing back injuries among nurses, for example, can have significant and direct effects on the organization's bottom line, Foulke says. And it's not just the reduced workers' comp costs because of fewer injuries, he says.

"When you reduce injuries, you dramatically increase efficiency and productivity, because you have that person on the job working instead of home recuperating," he says. "If that person gets injured and doesn't show up for work the next day, his or her productivity is zero, and the organization will spend money to cover for that loss of productivity. If you're eliminating that, you are achieving greater cost savings than just the massive savings in the workers' comp area. That's money right to the bottom line."

Risk management also contributes to the organization's public image, which is an important factor for hospitals and other providers in competitive environments, Foulke says. Worker injuries or deaths, as well as medical errors, can tarnish the hospital's reputation, which can drive away profitable patients, he says.

"The truth is that you cannot have great productivity, efficiency, and quality until you have great safety," Foulke says. "It's a one-way street. If you don't have good safety, people are getting injured, and that is going to impact your organization in all the ways that upper management . . . most focuses on. They will see it impact revenue, profitability, growth, all the important determinants of success, even if they don't read between the lines and see the impact of safety."

The risk manager should make it a priority to show that relationship, rather than hoping upper management will make the connection, Foulke says.

"Unfortunately, we see companies cut risk management and safety and health instead of realizing that they are the people who can help the company become more profitable, even when every other path is blocked," he says. ■

Present data the way C-suite wants it

When presenting any data to upper management, it is important to present it in the way that it will be best received, says **William Besse**, CHS-V, executive vice president of Andrews International, a company providing security and risk mitigation services, based in Valencia, CA. Every organization has its own culture, style, and business needs, and executives will expect data to be presented in the way they prefer and that works best within the organization.

"A large hospital corporation that owns hospitals across the country may have one way within their management structure of presenting data to their CEO or the board, and you had better present your data the same way the managers across the organization present their data," he says. "If it's visual, then do that. If it's all statistical analysis, then use that format. If it is an executive summary for the CEO and more details for others, do that."

Determine the style of communication long before it is time for you to walk into the board room, Besse says. If you do not present your information the same way as everyone else, it is not going to be accepted as widely as it could be, and you might not be recognized as someone making a meaningful contribution, he says.

Learn to speak C-suite

Risk managers also have to learn the language of the C-suite, says **Edwin Foulke Jr.**, JD, former assistant secretary of the federal Occupational Safety and Health Administration (OSHA) and now co-chair of the Workplace Safety & Catastrophe Management Practice Group with the law firm of Fisher & Phillips in Atlanta. *(See the story on p. 115 for Foulke's advice on positioning risk management as a profit center.)*

"You have to start talking the way they talk, things like 'return on investment,'" he says. "That's not something that is usually taught to risk managers, and it doesn't come naturally. But you have to be able to converse in the terms they understand, the terms that get their attention, if you want to be a part of the C-suite and have influence over budgeting and decision-making."

When interacting with organizational leaders at

this level, it also is important not to cry wolf too often, Besse says. Top managers will be sensitive to the possibility that a risk manager (or any other manager) is overstating a need or exaggerating a risk just to procure resources or elevate his or her status in the organization, he says.

"Overreaction to one particular incident can come back to hurt you in the end. It might have been just a black swan, an anomaly that no one could see coming, but you had the organization shift into high gear and spend, spend, spend in response to that one incident," Besse says. "Then that risk manager gets the reputation that you were taking advantage of the incident to obtain budget money or further your departmental goals, rather than supporting the enterprise as a whole. That can be a misstep."

SOURCES

• **Edwin Foulke Jr.**, JD, Co-Chair, Workplace Safety & Catastrophe Management Practice Group, Fisher & Phillips, Atlanta. Telephone: (404) 240-4273. E-mail: efoulke@laborlawyers.com.
• **William Besse**, CHS-V, executive vice president, Andrews International, Valencia, CA. Telephone: (661) 775-8400. ■

When do you notify after a HIPAA breach?

With the recent release of the HITECH rule's language on breach notification, risk managers can be left wondering when they have to notify after a breach of protected health information (PHI) in violation of the Health Insurance Portability and Accountability Act (HIPAA). Sometimes you should call the local newspaper and inform the Department of Health and Human Services (HHS), and sometimes you can just keep quiet.

EXECUTIVE SUMMARY

The federal government has changed the rule as to when you must notify after a breach of private health information under HIPAA. Providers now have some leeway in deciding, but it is not clear when notification is required.
• Some cases clearly require notification, such as when unencrypted data are lost in a public place.
• Other situations clearly do not require notification, such as when encrypted data are lost.
• Many situations will be unclear, so the provider has to weigh the consequences of notifying or not notifying.

So how do you know which path to follow? A close reading of the rule helps. The notification requirements for breaches and the potential penalties for noncompliance with HIPAA privacy rules were expanded under last year's HITECH Act. For HIPAA covered entities, a breach is defined as an event that "compromises the security or privacy of the protected health information," and defined further as posing "a significant risk of financial, reputational, or other harm to the individual."

That is not entirely clear, and the decision can be important. If you don't notify when you should, HHS will come after you. But if you notify when you really don't have to, you can create unnecessary stress for your patients and their families, and you could damage your hospital's reputation, all for nothing.

The changes to the breach notification rule give risk managers more flexibility but also create ambiguity. The HITECH rule finalized language that shows when notification is required after a breach of protected health information (PHI). Notice is required only if both of these conditions are met:

• There has been access to, or acquisition, use, or disclosure of PHI in violation of HIPAA.

• The violation poses a "significant risk of financial, reputational, or other harm" to the people whose PHI is involved.

• HHS states in the HITECH rule that a covered entity "will need to perform a risk assessment" to determine whether the second condition has been met but does not provide more guidance on how to make that decision.

HHS does make clear that you should be ready to justify your decision: "Covered entities and business associates must document their risk assessments so they can demonstrate, if necessary, that no breach notification was required."

(See the HITECH breach notification rule here: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/breachnotificationifr.html. See the HHS page on breach notification here: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html.)

The exact content of the information and the manner in which it was lost will determine whether you need to notify, says **Andrew Blustein**, JD, an attorney with the law firm of Garfunkel Wild in New York City. Not every breach will require a notification.

"If the information says Patient 123 has

a diagnosis of X, that is a HIPAA violation, because there is a patient identifier. But if someone finds that laptop and sees that information about Patient 123, with no name, you have to wonder if you've crossed that threshold," he says. "People seem to rush past what was actually disclosed and just panic over the fact that there has been a HIPAA breach."

In most cases, however, the breach will involve information that more clearly identifies the patient, Blustein says. And when the situation is not so clear, the burden is on the provider to show that the information posed no risk and required no notification.

"That's the risky part. When in doubt, you may have to go through the HITECH notification," he says. "If HHS comes in and looks at it, and if reasonable minds would differ, you're going to have to prove that your way was the reasonable way."

Blustein says the federal government's stance so far has been that if you have a name connected with a treatment, that is enough to trigger notification. That is not an official stance, he notes, but he says that has been the position of the investigators he has dealt with.

"Unfortunately, if you are in doubt, the best play is to play it safe and notify," he says. "Having the government come in and fine you, and tell you to notify patients now, is a very bad place to be. Then the institution can be seen in the light of not telling patients when things go bad, almost a coverup, and that's not what you want to be involved in."

Blustein says there is a move afoot to just require notification for all breaches, removing all ambiguity, but he says that would greatly increase the burden on health care providers. He recommends encryption as a way to avoid the problem altogether, because encrypted information never triggers the notification rule.

It is critical to understand exactly what information was compromised and how, says **Brian Lapidus**, chief operating officer with Kroll Fraud Solutions in Nashville, TN. He recently worked with a health care client who lost 2.2 million health care records, but he was able to prove that while the data was lost, there was no way the data could be accessed.

"The organization had no risk of harm and did not have to notify, because we could prove that the data was not accessible," he says. "Simply losing data is not the same as the data being compromised and accessible. A big question involves the intent and the circumstances of the lost [data], whether it was stolen by an angry employee or just lost somewhere. The forensic work can reveal a great deal about whether it is truly accessible to the public."

SOURCES

• **Andrew Blustein**, JD, Garfunkel Wild, New York City. Telephone: (516) 393-2218. E-mail: ablustein@garfunkelwild.com.

• **Brian Lapidus**, Chief Operating Officer, Kroll Fraud Solutions, Nashville, TN. Telephone: (615) 320-9800. E-mail: brian.lapidus@kroll.com. ■

Study: $20B in costs from medical errors

Findings from a new study indicate that measurable medical errors cost the U.S. economy $19.5 billion in 2008.

Commissioned by the Society of Actuaries (SOA) in Schaumberg, IL, and completed by consultants with Milliman in Seattle, the report used claims data to provide an actuarially sound measurement of costs for avoidable medical injuries. Of the approximately $80 billion in costs associated with medical injuries, around 25% percent were the result of avoidable medical errors, says **Jim Toole**, FSA, CERA, MAAA and managing director of MBA Actuaries, Inc.

"This report highlights a singular opportunity for both improving the overall quality of care and reducing health care costs in this country," Toole says. "Of the $19.5 billion in total costs, approximately $17 billion was the result of providing inpatient, outpatient, and prescription drug services to individuals who were affected by medical errors. While this cost is staggering, it also highlights the need to reduce errors and improve quality and efficiency in American health care."

Medical errors are a significant source of lost health care funds every year, he says. For example, the study found that $1.1 billion was from lost productivity due to related short-term disability claims, and $1.4 billion was lost from increased death rates among individuals who experienced medical errors. According to a recent SOA survey, which identified ways to bend the national health care cost curve, 87% of actuaries believe that reducing medical errors is an effective way to control health care cost

trends for the commercial population, and 88% believe this to be true for the Medicare population, says **Jonathan Shreve**, FSA, MAAA, consulting actuary for Milliman and co-author of the report.

"We used a conservative methodology and still found 5 million measureable medical errors occurred in 2008," Shreve says. "This number includes only the errors that we could identify through claims data, so the total economic impact of medical errors is in fact greater than what we have reported."

These were some key findings from the study:

- There were 6.3 million measureable medical injuries in the U.S. in 2008; of the 6.3 million injuries, the SOA and Milliman estimate that 1.5 million were associated with a medical error.
- The average total cost per error was about $13,000.
- In an inpatient setting, 7% of admissions are estimated to result in some type of medical injury.
- The measurable medical errors resulted in more than 2,500 avoidable deaths and more than 10 million excess days missed from work due to short-term disability.

"In the past, the insurance industry had low visibility in its involvement in quality-improving initiatives," says Toole. "Now is the time for the industry to assume an active role by helping health care systems implement an actuarial approach, which can more systematically identify potential causes of medical errors than alternative approaches."

The study also identifies the 10 medical errors that are most costly to the U.S. economy each year. Approximately 55% of the total error costs were the result of five common errors:

- pressure ulcers;
- postoperative infections;
- mechanical complications of devices, implants, or grafts;
- postlaminectomy syndrome;
- hemorrhages complicating a procedure.

The SOA and Milliman findings were based upon an analysis of an extensive claims database. Measureable costs of medical errors included increased medical costs, costs related to increased mortality rates, and costs related to lost productivity of an error.

For a full copy of the "The Economic Measurement of Medical Errors," report, go to http://www.soa.org/research/health/research-econ-measurement.aspx. ■

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 health care for hospital personnel to use in overcoming the challenges they encounter in daily practice. ■

COMING IN FUTURE MONTHS

■ Risk manager fired for whistleblowing

■ Language interpretation: Are you doing enough?

■ Hospitals try pilot program to reduce claims

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 **December** 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.

13. According to Mark Nelson, JD, an attorney with Drinker Biddle in Chicago, can private employers prohibit employees from using social networking sites?
A. Yes.
B. No.
C. It depends on state laws, and some states have laws that restrict an employer's ability to discipline or hold against an employee a lawful off-duty conduct in which the employee engages.
D. It depends on the state's constitutional protections.

14. Why does Timothy Folk, a partner with the Health & Human Services Industry Team at The Graham Company, a risk management consulting firm in Philadelphia, PA, say that workers' compensation is ideal for showing risk management's value to upper management?
A. Because it the most costly expense for most health care providers.
B. Because the frequency and severity of claims provides plenty of data for meaningful analysis.
C. Because it can be understood easily by those outside of risk management.
D. Because government data can be used to benchmark your performance.

15. When is notification required after a breach of PHI under HIPAA?
A. The violation poses a "significant risk of financial, reputational or other harm" to the people whose PHI is involved.
B. The violation poses a "possible risk of financial, reputational or other harm" to the people whose PHI is involved.
C. Always
D. Never

16. According to the study commissioned by the Society of Actuaries (SOA), how much did measurable medical errors cost the U.S. economy in 2008?
A. $19.5 billion
B. $30.6. billion
C. $50.5 billion
D. $3.2 billion

ANSWERS: 13. C; 14. B; 15. A; 16. A

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

Failure to Turn Woman Blamed for Pressure Sores and Death — $65,000 Illinois Verdict

by: **Radha V. Bachman**, Esq.
Buchanan, Ingersoll & Rooney, P.C.
Tampa, FL

Suzanne Gruszka, RN, MAS, CLNC, LHRM
Administrator, Clinical Support Services
Health Central
Ocoee, FL

News: A 76-year-old woman is taken to the hospital after collapsing at home. While at the hospital, the woman experiences an allergic reaction to the medications administered, resulting in a rash and blistering. Doctors ordered the woman to be turned every two hours to prevent pressure sores from forming. This course of treatment, however, was allegedly neglected, resulting in septicemia and eventual death.

Background: The plaintiffs brought this action on behalf of the decedent, a 76-year-old woman. Because of the woman's chronically low blood pressure, the decedent regularly took vasopressors, a powerful class of drugs intended to induce vasoconstriction, thereby elevating arterial pressure. Additionally, the woman was diagnosed as an uncontrolled diabetic and suffered from hypertension, coronary artery disease, and peripheral vascular disease. The woman collapsed while at home and was not discovered by her family for two days.

She was promptly rushed to the hospital, where she was diagnosed with emphysematous pyelonephritis in her left kidney. Emphysematous pyelonephritis is a severe necrotizing infection characterized by gaseous build-up typically caused by the *E. coli* bacteria. This systemic infection caused septic shock and multisystem organ failure. Additionally, upon arriving at the hospital, the woman suffered a partial myocardial infarction.

Four days after admission, the woman underwent surgery to remove the left kidney. As a result of this surgery and the aggressive treatment of her extremely low blood pressure, the woman gained 40 pounds of fluid during the first week following the surgery. Additionally, medications administered to the woman resulted in a severe allergic reaction, characterized by a bodywide rash and extensive blistering.

After one week of hospitalization, the nurses noted a tear in the skin over the sacrum and received consults from a dermatology service and a wound care team. The wound care team examined the woman's condition and ordered a specialty bed, a bowel management system, and ordered nurses to turn the woman every two hours to prevent further development of pressure sores.

Despite the wound-care physician's explicit instructions, the woman's pressure sores worsened, and she required three sharp debridements. These pressure sores rendered the woman septic, resulting in anoxic encephalopathy and recurrent mucous plugging of her tube.

The woman remained at the hospital before being transferred to another hospital. She remained at this second hospital for about one month before being transferred to a nursing home. The woman died several days after being transferred to the nursing home. The woman's death certificate listed coronary artery disease as the cause of death.

The plaintiffs, however, claimed that the death was ultimately the result of the pressure sores suffered while in the hospital's care. The plaintiffs claimed that the hospital's nursing staff failed to follow the wound care physician's instructions to

turn the woman every two hours. Additionally, the plaintiffs contend that the hospital's nutritionist failed to provide proper nutrition necessary to prevent and promote healing of the pressure sores.

The defendants claimed that the woman was turned every two hours, but that the hospital's staff failed to consistently chart the treatment. The defendants contend that the pressure sores were not caused by inadequate turning of the patient. Instead, the defendants claim the pressure sores were a result of the woman's severe edema and skin allergies. Finally, the defendants claimed that the death was not the result of a skin condition and noted that the woman's skin condition had been improving upon her discharge.

The case proceeded to the jury, and the jury awarded $65,000 against the defendants on the survival count.

What This Means to You: This is a case of a 76-year-old woman who suffered from multiple comorbidities, who had become ill at home, collapsed, and was not discovered for two days. Upon examination at the hospital, she is diagnosed with emphysematous pyelonephritis. This is a common infection in people with diabetes and can result in a severe and life-threatening condition if not recognized and treated promptly.

Among the bacteria associated with this infection, 66% of the time *E. coli* is isolated. The mean age of people with this type of infection is 55, and this condition is more likely to occur in women. Ninety-five percent of the patients have diabetes. A patient diagnosed with emphysematous pyelonephritis should be treated with aggressive medical management and possibly prompt surgical intervention, as necessary. Untreated, these cases result in death. Postoperative wound infection is common in these patients as wound healing is compromised.

Consequently, on presentation to the hospital, it was noted that the woman had suffered a myocardial infarction. It appears that she was stabilized and then underwent surgical intervention to remove her left kidney.

Postoperatively, the woman was treated with vasopressors for her low blood pressure and had become edematous, gaining 40 pounds of fluid after the surgery. She also had an allergic reaction to a medication that had been administered, which resulted in an overall bodywide rash and blistering. This condition of the skin, the edema, along with her history of diabetes, peripheral vascular disease, hypotension, and cardiovascular disease predisposed her for the development of pressure sores and poor wound healing overall.

Once the nurses identified a tear in the skin over the sacrum, the appropriate consults were obtained from both dermatology and the wound care team. The treatment prescribed was appropriate for the treatment of the developing pressure sore and the prevention of further skin breakdown. Unfortunately, the woman's pressure sores worsened, and she required debridements of the area(s). She eventually was diagnosed with sepsis.

The plaintiffs claim that the woman's death was due to the pressure sores she developed and that the nursing staff failed to follow instructions to turn the woman every two hours. The defendants state that the woman was turned every two hours, but that the hospital staff failed to document the intervention consistently in the medical record.

This discrepancy is unfortunately a common one, as nurses and staff often perform the ordered treatments or tasks, but do not necessarily document their interventions into the medical record. This gives the appearance of the treatment or task not being performed. This is a growing concern among hospitals and attorneys. How can you defend something that is not objectively documented? As hospitals embark on electronic documentation, this issue becomes greater. Documenting on a computer takes more time than documenting on paper, and unfortunately pertinent items get forgotten. There are many barriers to nursing documentation, whether on paper or electronically. It is impractical to carry the laptop or chart with you the entire shift, so nurses document retrospectively and rely on their recollection of the event, treatment, or task. The safety of medication administration has greatly improved using scanning devices, which document the administration by scanning the medication and the patient and matching both. The administration is immediately documented in the medical record. However, if the scanning device isn't working properly or the medication isn't scanning appropriately, work-arounds are employed, so that efficiency is not lost. This is where important information is lost, and patient safety is compromised.

Charting by exception has also been a controversial issue for the past 20 years. It leads the nurse to chart only if something unexpected happens. When retrospectively reviewing a medical record, it appears that no one was really assessing the patient. It goes back to something all nurses learn in training: "if it isn't documented, it wasn't done."

While it is understandable the defendants claim

that the patient's pressure sore development was due to her severe edema and skin allergies, the hospital staff did not adequately document their actions in response to the physician's orders, which violates the physician's orders and policies of this organization.

REFERENCE

Cook County (IL) Circuit Court, Case No. 06L-13360. ■

MD allegedly drunk at delivery: $2.5M verdict

News: A pregnant woman was admitted to the hospital for the delivery of her child. The on-call physician for her obstetrical group arrived and ruptured the woman's membranes. Following this, the physician allegedly began consuming alcohol. At the time of delivery, the baby suffered a fractured humerus. The physician then performed an episiotomy on the patient. The baby's injury healed, but evidence showed that problems with his growth plate could be the cause of future complications. The mother continues to have sexual dysfunction and pain after urination. The total jury verdict against all defendants was in the amount of $2,535,600.

Background: At full term, a woman was admitted to the hospital for the birth of her baby. The on-call physician from her obstetrical group arrived at the hospital and ruptured the woman's membranes. Shortly thereafter, it was reported that the physician traveled to a nearby park and began consuming alcohol. When the baby was ready for delivery, the physician encountered shoulder dystocia. Despite the physician's manipulations, the baby suffered a fractured humerus. After delivery was complete, the physician began performing an episiotomy on the woman for fourth-degree lacerations to the perineum. After completing the procedure, the physician was witnessed to be sleeping on a nearby stool in the delivery room. The grandmother of the infant could smell alcohol on the physician and made a scene at the hospital, excitedly announcing that the physician was drunk.

The hospital brought in the physician who handles impaired practitioners, and the physician submitted to an alcohol test, which resulted in the equivalent of a .22 blood alcohol content. The hospital required the physician to surrender his privileges the next day and notified the Kentucky Board of Medicine. The child's arm ultimately healed, but other physicians believed that problems with his growth plate as a result of the delivery could result in future complications. Likewise, the mother had ongoing issues with sexual dysfunction and bowel movements. The plaintiff claimed that the physician had a habit of drinking 1/5 of vodka on a daily basis and that his impaired state contributed to the injuries described. The plaintiff also alleged that the hospital was responsible for the injuries, because the nurses failed to protect the plaintiff against the impaired physician. The plaintiff admitted evidence that the nurses knew of the physician's drinking problem three weeks prior to the delivery, but the hospital did not conduct a proper investigation and alleged that the hospital's policies for recognizing and reporting impaired practitioners were inadequate. The "investigation" consisted only of a discussion with the physician and a report to his employer.

The physician argued that he had been sober for 30 days prior to the day in question but later admitted to drinking and denied any recollection of the delivery. The physician argued that the injuries to the baby were a result of the shoulder dystocia and not the physician's actions. The hospital defended by stating that the nurses did not have prior knowledge of the physician's drinking problems and only became aware of it following the delivery and that the hospital conducted a thorough investigation following the delivery. The hospital was found by the jury to be at 20% fault for the plaintiff's injuries.

The mother was awarded $5,000 in lost wages and $1.5 million for pain and suffering. The child was awarded $300,000. On punitive damages, addressed only as to the physician, the jury awarded a total of $700,000.

What This Means to You: This case centers on the actions of an impaired physician. The patient presented to the hospital in labor for the delivery of her child and was met by her obstetrical group's on-call physician, who ruptured her membranes. While the patient labored, it is noted that the physician began consuming alcohol.

The baby was delivered, suffering a fractured humerus due to shoulder dystocia. This is an obstetrical emergency that, if not treated promptly, can result in fetal demise due to the compression of the umbilical cord in the birth canal. Shoulder dystocia occurs in about 1% of vaginal births. Following shoulder dystocia deliveries, 20% of

babies will suffer some sort of injury, either temporary or permanent. The most common of these injuries are damage to the brachial plexus nerves, fractured clavicles, fractured humerus, contusions and lacerations, and birth asphyxia. A fractured humerus occurs in 4% of cases and heals rapidly.

The mother is also at risk when shoulder dystocia occurs. The most common complications are excessive blood loss and vaginal and/or vulvar lacerations. Such lacerations may involve the vaginal wall, cervix, extensions of episiotomies, or tears into the rectum.

Because of the pressure directed upward toward the bladder by the anterior shoulder in shoulder dystocia deliveries, post-partum bladder atony is frequently seen. Fortunately, it is almost always temporary. Occasionally, the mother's symphyseal joint may become separated or the lateral femoral cutaneous nerve damaged, most likely the result of overaggressive hyperflexion of the maternal legs during attempts at resolving the shoulder dystocia.

The literature does not definitively support an episiotomy unless it is necessary for the obstetrical maneuvers to deliver the fetus. It is therefore interesting that the physician performed an episiotomy on the woman after the delivery was complete. It appears she had already sustained a fourth-degree laceration and that an episiotomy would have been more appropriately performed at the time of delivery instead of after the completion of the delivery.

The case states that the woman's family noted alcohol on the physician's breath, and it would seem odd that the hospital staff did not identify this as well. It is not clear how and when the incident was reported; however, the alcohol level of .22 would lead one to believe that the hospital's administration and medical staff responded quickly to the incident. The hospital acted appropriately and reported the issue to the Kentucky Board of Medicine the following day.

The plaintiff presented evidence of habitual drinking and suggested that the nurses were aware of the physician's drinking three weeks prior to the delivery. It is alleged that the hospital did not conduct a proper investigation.

While the hospital and the medical staff may have been aware of previous instances of impairment, physicians are reluctant to report a colleague, because they do not want to do something that could end a colleague's career or have it backfire on them. Most physicians agree that if it meant that a patient could be injured or harmed in any way, they would report the impairment.

The AMA's Code of Medical Ethics is clear and states, "physicians have an ethical obligation to report impaired, incompetent, and unethical colleagues," and it lists several guidelines to follow. It recommends that before reporting an impaired physician to the state licensing board, physicians should first try to get the physician into a treatment program and/or to contact the hospital's chief of staff.

The reluctance to notifying state licensing boards is diminishing, as most boards will now refer impaired physicians who haven't injured patients to treatment programs without imposing sanctions on them. The problem is that it is often hard to spot impaired physicians before they harm patients. In academic hospitals, it is often difficult to hide an impairment. In a community hospital, it is far more difficult and much more identifiable.

In Kentucky, there is a physician recovery organization called the Kentucky Physicians Health Foundation. They have an Impaired Physicians program that originated in 1976 when the Kentucky Medical Association instituted the Impaired Physician Committee. The original committee performed on a voluntary basis as advocates for physicians who need help. In the 1980s, their focus was predominantly on helping physicians with alcohol and drug problems. The foundation continues today, and they currently monitor 125-160 physicians annually and average 40 new cases per year.

The Kentucky Board of Medical Licensure policy states that "if a licensed physician or hospital staff suspects that a physician is impaired-due to chronic alcoholism, chemical dependency, or physical/mental disability(ies)-such fact must be reported directly to the Kentucky Board of Medical Licensure within 10 days of obtaining direct knowledge of the impairment. Once the Board receives a report, they contact the physician and grant a 30-day grace period for the physician to contact the Impaired Physician Panel and to submit to an appropriate evaluation by the Foundation."

The verdict and award in this case appears appropriate. The physician knowingly took care of a patient while he was impaired. The delivery was a difficult one and involved an obstetrical emergency. While both patients survived, they may experience complications from the delivery for years.

Impaired physicians have been an issue for decades. Early identification and the reporting of impaired individuals can prevent potential death or serious harm to patients.

REFERENCE

Kenton County (KY) Circuit Court, Case No. 06-2827. ■