Healthcare Risk Management™

April 2011: Vol. 33, No. 4
Pages 37-48

IN THIS ISSUE

Financial Disclosure: Author **Greg Freeman**, Executive Editor **Joy Daughtery Dickinson**, Nurse Planner **Maureen Archambault**, Author **Radha V. Bachman**, and guest authors **Barbara Reding** and **Suzanne Gruszka** report no consultant, stockholder, speaker's bureau, research, or other financial relationships with companies having ties to this field of study. Guest author **Leilani Kicklighter** discloses that she is owner of the The Kicklighter Group and is course coordinator and lecturer on healthcare risk management at the University of South Florida.

AHC Media

Regulatory insurance: Worth the money, or not what it seems?

Cover regulatory liability, but is it too good to be true?

With providers facing potentially costly RAC audits and crackdowns on violations of everything from HIPAA and Stark to EMTALA, the idea of an insurance policy that will cover your fines and other costs can be quite appealing. But experts tell Healthcare Risk Management that you must be skeptical and consider all the fine print before paying that premium.

If the coverage sounds too good to be true, it probably is, they say.

The basic idea behind regulatory insurance is that the carrier will pay some or all of the expenses associated with audits and violations of government regulations: fines, penalties, legal fees, and other costs. Regulatory insurance coverage has been around for years, but it is getting more attention now because healthcare providers are feeling besieged by the federal government's efforts to root out fraud and abuse, says **R. Stephen Trosty**, JD, MHA, CPHRM, president of Risk Management Consulting in Haslett, MI. Trosty previously worked for an insurance company.

Insurance of this type can be a good investment, Trosty says. With the right type of policy, at the right price, regulatory insurance can take the sting out of a government investigation that finds wrongdoing, he says. If the policy covers legal expenses, that coverage alone can be worth the cost of the insurance, he says.

"When you have a government audit or investigation, even if you haven't

EXECUTIVE SUMMARY

Regulatory insurance is becoming more popular as the government increases audits and compliance oversight. The coverage can be a good idea for some providers, but be cautious in determining the value of a policy.

- Coverage is available for a wide range of regulatory infractions.
- Providers might be disappointed by exemptions and other limitations.
- Some jurisdictions don't allow insurance coverage for government-imposed penalties.

done anything wrong, the legal costs can break you," Trosty says. "One of the things you have to look at is whether the policy includes or excludes legal fees, because they vary. If you get one that excludes legal fees, it may not have the same value to you."

Many insurance companies offer regulatory insurance. The best place to start is with the company that already provides your other liability coverage for your health system, Trosty says. *(See the story on p. 39 for a description of one carrier's regulatory insurance product.)*

Deciding whether regulatory insurance makes sense for your organization can require a careful study of the policy and your risks. If your organization is involved with the purchase of hospitals, clinics, and physician groups, for example, the risk of a Stark violation increases. That's an argument in favor of regulatory insurance. "There are an increasing number of products offered, so there is more price competition now and the ability to negotiate is better," Trosty says. "I absolutely suggest that risk managers take a look at this type of coverage, especially as we see the number of audits increasing. As with any other financial risk, it is the responsibility of the risk manager to assess the risk, the likelihood of that risk actually happening, and do a cost benefit analysis."

That analysis might show that the coverage is worthwhile, though Trosty notes that some healthcare providers will find the cost can't be justified by the potential savings.

Read policy carefully

Watch out for the fine print that can dramatically affect the value of the policy. For example, some policies will have a maximum payout for a violation, whereas others might promise coverage for all expenses, Trosty says. Some policies might limit coverage to a certain number of violations or audits per year, he says.

Policies also might limit coverage for intentional violations, such as an employee stealing patient information.

"We're seeing more limitations in these policies now, with certain things being excluded and a cap of some sort on the amount to be paid or how many violations will be covered," Trosty says. "A lot of them will require a compliance program be in effect, and some will do an audit themselves to make sure there is some minimum protection, like the correct policies and procedures. Otherwise, most will deny you coverage, and the others will hit you with higher premiums and more exclusions."

Attorneys not sure of value

Health care attorneys tend to be skeptical about the value of regulatory insurance. **Jonathon E. Cohn**, JD, a partner in the health care practice of law firm Arent Fox in Los Angeles, says clients

Healthcare Risk Management® (ISSN 1081-6534), including HRM Legal Review & Commentary™, is published monthly by AHC Media, a division of Thompson Media Group 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 105109, Atlanta, GA 30348.

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 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.
Executive Editor: **Joy Daughtery Dickinson** (229) 551-9195 (joy.dickinson@ahcmedia.com).
Production Editor: **Neill L. Kimball**.

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

have been asking him about these products, but that he cautions them to be careful.

The products he has seen concern him because they offer limited coverage with lots of exclusions, he says. Considering the cost of premiums, Cohn often advises health care providers that they would be better off to self-insure.

"I'm not particularly impressed by the products I've seen," Cohn says. "What you need in a policy like this is the obligation to defend and the obligation to indemnify. I've seen products where the carrier does not indemnify and will reimburse attorney fees, which isn't the same as providing a defense, with the attorney fees capped at about $25,000. You're not getting much."

Last year Cohn worked with a chain of nursing facilities that was considering regulatory insurance, and he told them not to buy it. Once he sorted through the limitations, the policy wasn't worth the premium, he told the client. "This one offered indemnification along with the defense, so it looked promising," he says. "But there were so many carveouts and exemptions for the indemnification that I thought the policy was very, very limited."

Coverage not valid in some areas

Regulatory insurance also raises a public policy question that has yet to be resolved in states such as California, which only recognizes insurance coverage for certain things. California does not recognize insurance coverage for crimes or wrong dealings, so fraud and abuse coverage would be unenforceable since it would be against California law to insure against that kind of loss.

"Even if your state allows this coverage, the insurer is not going to pay for intentional misdeeds, and they'll be looking for a way to call it intentional. So if you have a violation, you're going to get a reservation of rights letter that says maybe they'll pay if it was negligence, but if it wasn't you're on your own," Cohn says. "When you're expecting a check, you might get a runaround instead."

Similar concerns come from **George B. Breen**, JD, an attorney with the law firm of Epstein Becker Green in Washington, DC. Breen is co-chair of the Health Care and Life Sciences Litigation and Government Investigations Practice Group. "The carriers like to focus on the penalties, but the penalties often are not the cost driver, as it is the associated costs in dealing with the breach," Breen says. "You may pay a $250,000 fine but have $7 million in business costs resulting from the HIPAA violation or other breach."

With a RAC audit, for example, Breen notes that challenging the audit results can be a long and expensive process involving several steps in the appellate courts before the district court. The costs associated with the appeal might not be covered, or they might consume the total value of the policy.

If the policy provides for a defense, Breen also advises checking the details to determine who has the authority to choose the attorney and whether the carrier can settle the case without your approval.

There is no one answer to whether regulatory insurance is worthwhile, Breen says. The coverage tends to be a better fit for smaller health care providers, such as physician groups, than for large hospitals or health systems, he says. Government penalties can be more damaging to a smaller provider, which can argue in support of the premium.

"If you find the right policy at the right price, you might decide that it gives you enough peace of mind that you're willing to pay the premium," he says. "But I worry that a lot of health care providers are going to pay for coverage like this and then find out it is of limited utility, when you look at all the costs involved with an incident."

SOURCES

• **George B. Breen**, JD, Attorney, Epstein Becker Green, Washington, DC. Telephone: (202) 861-1823. E-mail: gbreen@ebglaw.com.
• **Jonathon E. Cohn**, JD, Partner, Arent Fox, Los Angeles. Telephone: (213) 443-7515. E-mail: cohn.jon@arentfox.com.
• **R. Stephen Trosty**, JD, MHA, CPHRM, President, Risk Management Consulting, Haslett, MI. Telephone: (517) 339-4972. E-mail: strosty@comcast.net. ■

Insurance is inexpensive, and it can be retroactive

Regulatory insurance is becoming more popular with health care providers, says **Chip Goen**, vice president of sales with MAG Mutual Insurance Agency (MMIA) an insurance company in Atlanta. The company writes about 10 regulatory policies a month, up significantly over the past few years.

MMIA offers regulatory insurance that is retroactive for six years, with legal representation and coverage for audits, fines, and penalties. The policy would cover the cost of hiring an independent auditor to conduct a "shadow audit" alongside RAC or other auditors, Goen says.

The policy covers HIPAA, EMTALA, and Stark investigations, as well as audits and commercial payer inquiries. Restitution for overbilling is not covered, Goen says.

Policy caps will vary depending on the provider. A solo physician's cap would be $1 million, for instance, but a large practice or hospital would have a limit of $5 million, he says.

"The underwriters love to see a compliance program in effect, and they do give premium credits to small practices for having one," Goen says. "It would be a requirement for a hospital or a large practice, but not for smaller providers."

The regulatory insurance product is getting more attention because providers are realizing that "it's not a matter if they're going to get audited; it's a matter of when," Goen says.

Coverage costs about $1,000 per year per physician in a practice group. Hospital premiums are determined by the number of beds and annual revenue. A 300-bed hospital probably would pay about $50,000 per year for coverage, he says.

SOURCE

• **Chip Goen**, Vice President, Sales, Mag Mutual Insurance Agency, Atlanta. Telephone: (404) 842-5584. E-mail: cgoen@magmutual.com. ■

Shocker: First civil penalty for HIPAA violation

The first civil monetary penalty handed down by the Department of Health and Human Services (HHS) has created a buzz throughout the health care industry, and not just because of the eye-popping amount of the fine: $4.3 million.

As shocking as the size of the penalty is the nature of the alleged violation. HHS didn't impose its first, precedent setting fine for any grand scheme to steal patient information and profit somehow from its commercial use. The $4.3 million penalty was imposed for failing to give patients access to their own information when they asked.

The HHS Office for Civil Rights (OCR), the arm that enforces HIPAA, imposed the civil monetary penalty against Cignet Health, a group practice and clinic in Temple Hills, MD, for violating the HIPAA Privacy Rule. Although there have been a number of settlements arising from alleged HIPAA violations, never before has OCR imposed a civil monetary penalty against a covered entity for violating the HIPAA Privacy Rule, explains **Lawrence W. Vernaglia**, JD, a health care attorney with the law firm of Foley & Lardner in Boston and chair of the firm's Health Care Industry Team.

The penalty against Cignet was based on the new violation categories and the increased penalty amounts authorized by the Health Information Technology for Economic and Clinical Health (HITECH) Act. OCR's action might foreshadow increased scrutiny and an invigorated willingness to assess significant penalties against covered entities for HIPAA violations, Vernaglia says. *(For more on HITECH, see "HITECH, meaningful use bring concerns for risk manager,"* Healthcare Risk Management, *September 2010, p. 97.)*

HHS flexing its muscle

The $4.3-million civil monetary penalty was triggered by Cignet's failure to provide access to the medical records of 41 patients, as well as its failure to adequately cooperate with OCR's investigation, according to information released by HHS. *(See the story on p. 41 for more details of the alleged violations and OCR's investigation. See the story on p. 42 for a recent settlement of HIPAA charges.)*

At a press conference held to announce the groundbreaking penalty, HHS Secretary Kathleen Sebelius made clear that the department is not playing around. "Ensuring that Americans' health information privacy is protected is vital to our health care system and a priority of this admin-

EXECUTIVE SUMMARY

The Department of Health and Human Services (HHS) has imposed the first civil monetary penalty for HIPAA violations on a group practice. The company was fined $4.3 million for failing to provide access to the medical records of 41 patients.

- The penalty was large considering the type of alleged violation, a lawyer says.
- The large fine is seen as a warning to other providers.
- HHS contends the provider ignored letters from the department.

istration," Sebelius said. "The U.S. Department of Health and Human Services is serious about enforcing individual rights guaranteed by the HIPAA Privacy Rule."

OCR Director **Georgina Verdugo**, JD, LLM, MPA, said the company's "arrogance" was a primary reason for the large penalty. "Covered entities and business associates must uphold their responsibility to provide patients with access to their medical records and adhere closely to all of HIPAA's requirements," Verdugo said. "The U.S. Department of Health and Human Services will continue to investigate and take action against those organizations that knowingly disregard their obligations under these rules."

Cignet Health did not return calls seeking comment.

Not what was expected

Vernaglia says he was initially "astonished" by the amount of the penalty. He expected that such a huge fine would have been the result of a health care provider selling patient information to marketers, a brazen violation of HIPAA.

"It was too much money for the alleged violations underlying it, way too much for failing to give access to patient records," he says. "But the more I understood what happened, I realized it was a lot more about being unresponsive to the government when they came asking questions about it."

According to HHS, the company even failed to comply with a federal subpoena ordering it to produce the records.

Cignet Health's resistance to the government inquiries is puzzling, Vernaglia says. In particular, he wonders what was going through the mind of the physician to whom all of the HHS correspondence was addressed. "It's possible that this person had too much on his plate and just ignored the HHS letters, hoping they would go away," he says. "But it could be that the letters were all addressed to him and he wasn't even there, so they just never got anyone's attention. It would explain at least the initial failure to respond."

Lessons for risk managers

Some type of systems or process failure, or multiple failures, must have caused the problems at Cignet Health, Vernaglia says, because it is inconceivable that the company would have willfully ignored the government investigation. Vernaglia says there are several lessons from the case for risk managers:

- Covered entities should examine their current HIPAA policies and practices, including their compliance program provisions for responding to requests for access to medical records, to verify that the entity's operations are current with the recent legal changes.
- Cooperate fully with HHS investigations, even if you feel the allegations are unjust or trivial.
- Misdirected communication can lead to disaster. Make certain you have a system in place to ensure that any such communication from HHS or another government entity is directed to the correct person, opened immediately, and forwarded to legal counsel as necessary. Update policies and procedures frequently to ensure such items are directed to the right person.
- HHS is willing to impose hefty penalties for what might seem like minor violations of HIPAA. If you are only watching out for the big willful violations of HIPAA, you could be hit hard for violations that seem like a small matter.

"A good compliance program could have made this a very different kind of case," Vernaglia says. "Even if they failed to produce records for the patients, the fine in the end would have been several magnitudes smaller. HHS is giving them a spanking, and that's what you get when you ignore the government."

SOURCE

• **Lawrence W. Vernaglia**, JD, Foley & Lardner, Boston. Telephone: (617) 342-4079. E-mail: lvernaglia@foley.com. ■

HHS: First they ignored patients, then ignored us

The $4.3 million civil monetary penalty imposed on Cignet Health in Temple Hills, MD, could have been avoided by simply responding to the reasonable requests of patients for their own medical records, according to the case laid out by the Department of Health and Human Services (HHS).

And even after failing to do that, Cigna could have saved itself a lot of grief by responding to numerous letters from HHS and cooperating with the investigation. Instead, they just kept digging the hole deeper, HHS says.

In a Notice of Proposed Determination issued Oct. 20, 2010, HHS Office for Civil Rights (OCR) found that Cignet violated 41 patients' rights by denying them access to their medical records when requested between September 2008 and October 2009. These patients individually filed complaints with OCR, initiating investigations of each complaint. The HIPAA Privacy Rule requires that a covered entity provide a patient with a copy of their medical records within 30 (and no later than 60) days of the patient's request. The civil monetary penalty for these violations is $1.3 million per incident.

During the investigations, Cignet refused to respond to OCR's demands to produce the records, OCR Director Georgina Verdugo, JD, LLM, MPA, said at a conference. Additionally, Cignet failed to cooperate with OCR's investigations of the complaints and produce the records in response to OCR's subpoena, she said. OCR filed a petition to enforce its subpoena in United States District Court and obtained a default judgment against Cignet on March 30, 2010.

On April 7, 2010, Cignet produced the medical records to OCR, "but otherwise made no efforts to resolve the complaints through informal means," according to HHS documents.

OCR also found that Cignet failed to cooperate with OCR's investigations on a continuing daily basis from March 17, 2009, to April 7, 2010, and that the failure to cooperate was due to Cignet's willful neglect to comply with the Privacy Rule. Covered entities are required under law to cooperate with the department's investigations. The civil monetary penalty for these violations is $3 million. The final determination and penalty was announced Feb. 22, 2011.

A copy of the Notice of Proposed Determination and Notice of Final Determination can be found at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/cignetpenaltynotice.pdf. ■

Documents left on subway led to $1 million in fines

A large hospital system in Massachusetts has agreed to pay $1 million in fines and improve its policies and procedures after an employee left patient information on a subway.

The General Hospital Corp. and Massachusetts General Physicians Organization (known collectively as Mass General) have agreed to the penalty and corrective action plan (CAP) to settle potential HIPAA violations, the Department of Health and Human Services (HHS) announced.

Mass General, one of the nation's oldest and largest hospitals, signed a Resolution Agreement with HHS that requires it to develop and implement a comprehensive set of policies and procedures to safeguard the privacy of its patients. The settlement follows an extensive investigation by the HHS Office for Civil Rights (OCR), which enforces HIPAA, said OCR Director **Georgina Verdugo**, JD, LLM, MPA.

"We hope the health care industry will take a close look at this agreement and recognize that OCR is serious about HIPAA enforcement," Verdugo said. "It is a covered entity's responsibility to protect its patients' health information."

The incident giving rise to the agreement involved the loss of protected health information (PHI) of 192 patients of Mass General's Infectious Disease Associates outpatient practice, including patients with HIV/AIDS. OCR opened its investigation of Mass General after a complaint was filed by a patient whose PHI was lost on March 9, 2009.

OCR's investigation indicated that Mass General failed to implement reasonable, appropriate safeguards to protect the privacy of PHI when removed from Mass General's premises and impermissibly disclosed PHI, potentially violating provisions of HIPAA.

The impermissible disclosure of PHI involved the loss of documents consisting of a patient schedule containing names and medical record numbers for 192 patients, and billing encounter forms containing the name, date of birth, medical record number, health insurer and policy number, diagnosis, and name of providers for 66 of those patients. These documents were lost on March 9, 2009, when a Mass General employee, while commuting to work, left the documents on the subway train that never were recovered, according to the HHS investigation.

Details of corrective action plan

Mass General also agreed to enter into a CAP that requires the hospital to:

- develop and implement a comprehensive set of policies and procedures that ensure PHI is protected when removed from Mass General's premises;

• train workforce members on these policies and procedures;

• designate the director of internal audit services of Partners HealthCare System to serve as an internal monitor who will conduct assessments of Mass General's compliance with the CAP and render semi-annual reports to HHS for a three-year period. ■

Patient safety and metrics: Obtain good data

Risk managers are collecting data and using metrics in many ways lately, and patient safety should be a primary focus, says **David G. Danielson**, JD, CPA, senior vice president of clinical risk management at Sanford Health in Sioux Falls, SD.

Patient safety can be improved by the use of metrics, but that improvement first depends on having good data, Danielson says. He recommends, at a minimum, that providers collect data related to the National Quality Forum's Safe Practices for Better Healthcare -- 2010 Update. *(The safe practices guide is available at www.qualityforum.org/About_NQF/CSAC/Safe_Practices_Table.aspx.)*

"Tracking and trending will help a system identify potential problems. From there, solutions can be developed," Danielson says. "The key is the implementation of the solutions. An organization must have both the awareness and the capability to make solutions stick. This is heavy work, as the inertia of the status quo fights against the changes."

Metrics can help isolate the problems, making it possible to correct them and improve patient safety, Danielson says. "We regularly hold multicausal analysis forums to look for ways we can improve our clinical practice," he says. "I use the data to change policies and procedures, talk with clinical departments and providers, and report to senior management about improving safety for our staff and patients."

Danielson and his colleagues did just that with a medication reconciliation project. The pharmacy was able to gather data about the types and locations of drug variances, and that information was presented to senior management. The senior managers authorized an education program about the importance of making sure there was a correct listing of each patient's medications. "Using the data, we focused on both the higher risk areas as well as those areas with higher variances," he says. "After the education, we again tracked and trended the variances and we have improved."

Useful information can be obtained by performing a root cause analysis or failure mode analysis when an adverse event occurs, to find out what went on behind the event, says **Alan Rosenstein**, MD, MBA, medical director of Physician Wellness Services, a company in Minneapolis that provides services to troubled physicians and their employers. "The analysis often finds that there were failures in communication and/or collaboration," he says.

Rosenstein notes that, according to The Joint Commission, 65% of sentinel events can be traced back to an error in communication. When performing post-event analysis, risk managers need to evaluate the contribution of human factor issues as well as structural process issues. Then the risk manager should look for solutions that will address communication gaps to prevent an unwanted reoccurrence of a potentially preventable adverse event, he says.

"Additionally, it is important to implement standard patient safety and quality indicators in each department or area with measurements specific to each department or area," Rosenstein says.

An indirect measure of patient safety and quality is patient satisfaction, Rosenstein notes, which can be determined through surveys. In such a survey, include questions that address the patient's comfort and the ability to interact with providers and obtain the information they thought was necessary to understand their situation and make the right decisions, he says. Research has shown that poor patient satisfaction correlates with higher medical malpractice risk, he says.

These surveys also can be extended to an organization's staff to determine safety culture and staff satisfaction, he suggests. "These surveys should include questions based around specific behaviors and perceptions around communication and collaboration," Rosenstein says. "Poor communication and collaboration are strongly linked to adverse events and outcomes." One example of a survey question that can help evaluate the safety culture is "How would you rate the effectiveness of physician communication/ nurse communication in helping you understand your medical condition?"

Change sometimes can best be achieved by addressing the "human factor" issues at the individual level through education for all staff members to encourage and facilitate better communication and improved collaboration between team members, he says.

"The education should raise the level of awareness of what disruptive and unprofessional behaviors are and how they can negatively impact work relationships, communication flow, and team collaboration, and how they can adversely impact outcomes of patient care," Rosenstein says. "Stress the importance of holding individuals accountable for their actions. Provide workshops on improving communication skills. Stress the importance of timely intervention, coaching, and counseling, and if needed, more comprehensive interventions."

Coaching also helps individuals understand what they are doing to impede patient safety and also helps improve staff member performance. Examples would be helping individuals see how their behaviors might be perceived by others (raising emotional intelligence), and providing tools and techniques that will help them deal appropriately with factors affecting their behaviors. Additionally, an intervention might be necessary for individuals who are non-compliant or whose actions pose an immediate risk to patient safety, he says.

Rosenstein's company once helped coach a physician who was perceived as "hotheaded" and "unapproachable" by his physician peers. He described himself as passionate and committed and was resistant to change. He failed to see how his "message" was consistently misinterpreted or lost totally due to his delivery of the message, Rosenstein says.

Through coaching he was able to increase his awareness of how his delivery of messages was destructive vs. constructive, recognize how to better manage the day-to -day stress and frustration inherent in clinic practices, and more selectively choose the issues he felt strongest about. He realized he had been regularly asked to "carry the flag" on behalf of his colleagues he were unwilling to bring the issue forward, which he stopped doing.

The coaching helped the physician engage in a process of consciously identifying "new behavior" vs "old behavior" and intentional efforts to gravitate toward "new behaviors."

"In any of these instances, having hard data through capturing these metrics will create a much more compelling case for change," he says.

SOURCES

• **David G. Danielson**, JD, CPA, Senior Vice President of Clinical Risk Management, Sanford Health, Sioux Falls, SD. Telephone: (605) 333-6556. E-mail: david.danielson@sanfordhealth.org.
• **Alan Rosenstein**, MD, MBA, Medical Director, Physician Wellness Services, Minneapolis, MN. Telephone: (888) 892-3861. E-mail: alan.rosenstein@workplacebehavioralsolutions.com. ■

Stop identify theft — Spend more on security?

One-third of providers say their organization has had at least one known case of medical identity theft, and some of those cases might not have been reported, according to a recent survey by the Healthcare Information and Management Systems Society (HIMSS).

The survey interviewed 272 IT and security professionals at hospitals and medical practices. Now in its third year, the 2010 HIMSS Security Survey, sponsored by Intel, reports the opinions of information technology (IT) and security professionals from health care provider organizations across the country regarding key issues surrounding the tools and policies in place to secure electronic patient data at health care organizations.

The rate of medical identity theft is surprising to **Eduard Goodman**, JD, a privacy lawyer and chief privacy officer for Identity Theft 911, a company in Scottsdale, AZ, that provides data protection and similar services. He was surprised that health care providers still are facing so much identity theft even with significant HIPAA penalties hanging over their heads.

"HIPAA is one of the few areas of law in which the injury is just the release of the information

EXECUTIVE SUMMARY

Medical identity theft has occurred in one-third of health care facilities, according to new survey results. Some providers report that they are beefing up security in response.
• More than half of the respondents conduct a formal risk analysis annually.
• Some providers are spending more of their IT budgets on security.
• Encryption is becoming more common.

itself. It's not about whether anyone uses that information to commit a crime," Goodman says. "With that in mind, you would expect providers to work harder to protect that data, and a third are saying they've failed on that point."

Not all conducting risk analyses

The security data is particularly important for providers trying to meet the meaningful use objectives. How do you measure up against your peers?

The Electronic Health Record Incentive Program identifies 14 meaningful use objectives for eligible hospitals and 15 core meaningful use objectives for eligible professionals. (The final rule is available at http://edocket.access.gpo.gov/2010/pdf/2010-17207.pdf. The language describing the objectives and measures is on pages 19-57, and a grid that identifies each objective and measure is on pages 58-63.) Meeting those objectives is required to receive funds for transitioning to electronic health records provided through the new Medicare and Medicaid incentive program.

Additionally, hospitals and eligible providers also must focus on five of 10 menu set objectives to quality for incentive funds. One of these rules specifically stipulates that they must protect electronic health information created or maintained by the electronic health record (EHR) by conducting or reviewing a security risk analysis. These organizations also must implement security updates as necessary and correct identified security deficiencies as part of their risk management process. Risk analysis is a key requirement of the Health Insurance Portability and Accountability Act (HIPAA) final security rule, and as such, has been a requirement for health care organizations for many years.

Results from the 2010 HIMSS Security Survey indicated that three-quarters of all respondents reported that they perform a risk assessment at their organizations. "While this is similar to the percentage reported last year, this year's study has a greater representation of medical practices, and there is a clear difference in the percent of respondents that indicated they conducted a risk analysis," the report says. "Respondents working for medical practices were twice as likely to report that their organization does not conduct a risk analysis compared to those that work at a hospital (33% compared to 14%)." *(See story, right, for more results from the survey.)*

Quarter wouldn't qualify now

The meaningful use criteria states that not only are organizations required to conduct a risk analysis, but they also must correct deficiencies identified during the risk analysis process.

"At present, one-quarter of the sample population would not qualify for meaningful use," the report states. "In addition, establishing a robust security environment is crucial as hospitals and medical practices increasingly share information outside of their organizations."

Overall, a high percentage of those that are conducting a risk assessment reported using this information to determine which security controls should be put into place at their organizations. The risk assessment results also were used by many organizations to identify gaps in existing security controls, policies, and/or procedures. As a result of the risk assessment, organizations were able to actively take steps to correct deficiencies. The survey data serves to emphasize the important role and value that ongoing security risk analysis can play in protecting health data.

The risk analysis is particularly important as providers move toward EHRs, Goodman says.

"I think people are truly underestimating the level of security and diligence that will have to go into protecting those electronic records," Goodman says. "When someone tries to steal 200 paper records with health information, that's a couple of boxes at least. Now you'll have thousands on a thumb drive, and that convenience makes them that much easier to steal. More portable for you means it's more portable for a thief, too."

SOURCE

• **Eduard Goodman**, JD, Chief Privacy Officer, Identity Theft 911, Scottsdale, AZ. Telephone: (888) 682-5911. E-mail: egoodman@idt911.com. ■

Most hospitals have full-time risk assessments

These were some key results from the recent survey conducted by the Healthcare Information and Management Systems Society (HIMSS):

Medical identity theft: One-third of respondents

reported that their organization has had at least one known case of medical identity theft at their organization. Those working for a medical practice were much less likely to report that an instance of medical identity theft occurred at their organization (17%), when compared to those working for a hospital organization (38%).

Patient identity: Half of respondents indicated that they validate patient identity by requiring a government/facility-issued ID and checking the ID against information in the master patient index. A similar percent reported that they have a formal process for reconciling duplicate records in their master patient index.

Maturity of environment: Respondents characterized their environment at a middle rate of maturity, with an average score of 4.43 on a scale of 1 to 7, where one is not at all mature and seven is a high level of maturity. Maturity refers to the organization's adoption of security measures.

Security budget: About half of respondents reported that their organization spends 3% or less of their organization's IT budget on information security. However, while this was consistent with what was reported last year, many respondents indicated that their budget actually increased in the past year, primarily as a result of federal initiatives. There is little difference in response in this area by organization type.

Formal security position: Slightly more than half (53%) of respondents reported they have a chief security officer or full-time staff in place to handle their organizations' security function. Those working for a hospital were more likely to report that they had a chief security officer in place compared to individuals working for medical practices. Also, while 17% of respondents working for medical practices indicated that they handled their security function exclusively using external resources. None of the respondents from the hospitals reported that they used external resources exclusively.

Risk analysis: Slightly more than half of respondents (59%) that reported that their organization conducts a formal risk analysis indicated that this type of analysis is conducted annually. Susceptibility to internal threats and external threats are nearly universally included in the risk analysis.

Patient data access: Surveyed organizations most widely use user-based and role-based controls to secure electronic patient information. User-based security requires the user to log on with credentials such as a username and password, whereas role-based security restricts access to authorized people in certain roles. More than half of respondents from hospital organizations reported that they used two or more types of controls to manage data access, compared to 40% percent of respondents from medical practices. About half of respondents reported that their organization allows patients/surrogates to access electronic patient information.

Management of security environment: Nearly all respondents reported that their organization actively works to determine the cause/origin of security breaches, and two-thirds reported having a plan in place for responding to threats or incidents related to a security breach. Respondents working for the hospital organizations in this sample were more likely to report that they worked to determine the cause/origin of security breaches than were their counterparts at medical practices.

Security in a networked environment: About 85% of respondents reported that their organization shares patient data in an electronic format. Data is most frequently shared with third party providers, state government, third party providers and other facilities within the corporate organization. While respondents from hospitals are somewhat more likely to report (83%) that they will share data in the future than are those from medical practices (77%), the likelihood of data sharing in the future is high among both groups.

Future use of security technologies: Mobile device encryption, e-mail encryption, and single sign on and were most frequently identified by respondents as technologies that were not presently installed at their organization but were planned for future installation. Respondents from hospitals that were not presently using these technologies are more likely to report expectations that they would install them in the future, compared to respondents in medical practices. ■

1/3 of imaging costs defensive, study says

Pennsylvania research eyes orthopedics

Nearly 35% of all the imaging costs ordered for 2,068 orthopedic patient encounters in Pennsylvania were ordered for defensive purposes, according to study presented recently at the 2011

Annual Meeting of the American Academy of Orthopaedic Surgeons (AAOS).

It is well known that physicians order diagnostic procedures that are of little or no benefit to a patient, largely to protect themselves from a lawsuit. Until now, however, efforts to actually measure defensive medicine practices have been limited primarily to surveys sent to physicians. Such surveys simply would ask whether or not that individual actually practiced defensive medicine, explains **John Flynn**, MD, associate chief of orthopedic surgery at Children's Hospital of Philadelphia and author of the study.

"This is the first study we know of that looked at the actual practice decisions of physicians regarding defensive imaging in real time, prospectively done," Flynn says.

Many lawsuits hinge on the plaintiff's lawyer's claim that the doctor should have ordered extra diagnostic testing, and that claim is the driving force behind much of the defensive test ordering, he says.

Specifics of the study

Seventy-two orthopedic surgeons, who are members of the Pennsylvania Orthopaedic Society, voluntarily participated in the study, which included some 2,068 patient encounters throughout the state. Most patients in the study were adults. The study found that 19% of the imaging tests ordered were for defensive purposes. Defensive imaging was responsible for $113,369 of $325,309 (34.8%) of total imaging charges for the patient cohort, based on Medicare dollars. The overall cost of these tests was nearly 35% of all imaging ordered because the most common test was an MRI, an imaging test which costs more than a regular X-ray.

The legal environment that drives physicians to order additional tests has an effect on patients too, in a way that involves more than costs, Flynn says. "Patients are sometimes put through tests that maybe otherwise would not be ordered," he says.

The finding from this research that surprised Flynn the most was that surgeons were more likely to practice defensively if they had been in practice for more than 15 years. "This was counterintuitive," he says. "I thought that young doctors would come out of medical school immediately after training, be less confident because they weren't experienced, and order more defensive tests. Then, as they become more comfortable and confident after 10 or 20 years in practice, they would order many fewer tests."

In fact, the opposite was true. Flynn found that, in Pennsylvania at least, a surgeon's defensive nature grows worse over time. In this legal environment, orthopedic surgeons order more imaging tests of a defensive nature, because over time they become more concerned that someone is going to second guess or sue them.

"Ideally, as a next step, we would hope to try to get a broader national picture using this prospective practice audit methodology, so we could get a better sense of the true costs of defensive imaging in orthopedics," Flynn says. "Ultimately, if you had doctors from multiple specialties, from OB/GYN to neurosurgery to emergency medicine, do this type of practice audit, you could accurately quantify how much of our nation's health care resources are wasted on defensive medicine."

SOURCE

• **John Flynn**, MD, Associate Chief of Orthopedic Surgery, Children's Hospital of Philadelphia. Telephone: (215) 590-1000. ■

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

■ Hospital revamps procedures after wrong-site

■ Improving ED call coverage — the latest ideas

■ Insurer focuses on OB training to reduce med mal

■ Anesthesia drugs diverted for murder

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 letter of credit. When your evaluation is received, a credit letter will be mailed to you.

12. What does R. Stephen Trosty, JD, MHA, CPHRM, president of Risk Management Consulting, say is the current trend with regulatory insurance?
A. There are more limitations in the policies now, with certain things being excluded and a cap of some sort on the amount to be paid, or how many violations will be covered.
B. There are fewer limitations in the policies now, with insurers more willing to provide coverage of all expenses related to an audit or infraction.

13. Does a provider have to have a compliance program in place to qualify for the regulatory insurance offered by MAG Mutual Insurance Agency?
A. Yes, all providers must have a compliance program to qualify.
B. No, the carrier does not require a compliance program for any provider.
C. A compliance program is required for a hospital or a large practice, but not for smaller providers.

14. According to the Department of Health and Human Services, what did Cignet Health do that yielded a $4.3 million civil monetary penalty?
A. Cignet provided private patient information to a marketer in exchange for payment.
B. Cignet lost the records of 4,000 patients in an unencrypted format.
C. Cignet failed to comply with a previous agreement to improve its compliance program.
D. Cignet failed to provide access to the medical records of 41 patients, and it failed to adequately cooperate with the Office for Civil Rights' investigation.

15. Which of the following was a finding of the 2010 Healthcare Information and Management Systems Society (HIMSS) Security Survey?
A. One-third of respondents reported that medical identity theft had occurred at their institutions.
B. Most respondents said their IT security budgets had tripled in the past year.
C. Almost none of the respondents reported that medical identity theft had occurred at their institution.

ANSWERS: 12. A; 13. C; 14. D; 15. A

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

Woman involuntarily committed suffers mental anguish — $65,000 verdict awarded

By **Radha V. Bachman**, Esq.
Buchanan, Ingersoll & Rooney, PC
Tampa, FL, and

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

News: A woman suffering from personal problems and the subsequent unexpected death of her son was involuntarily committed to a behavioral health center by a psychologist allegedly following a telephone conference in which the woman expressed suicidal ideation. The physician failed to document the specifics of the conversation on the records required for an involuntary commitment. The woman sued the physician and the center. A Louisiana jury found that the applicable standard of care had been breached and awarded the woman $65,000 in damages.

Background: A 28-year-old single woman went to visit a clinical psychologist complaining of stress reaction and some bouts of marital discord. Shortly after the visit, the woman's son passed away unexpectedly in an accident. After the son's funeral, the psychologist engaged in a telephone conference with the woman and allegedly determined that the woman expressed suicidal ideation. Following the telephone conference, the woman was involuntarily committed to a behavioral health center in the area. The woman remained in the center for nine days.

The woman asserted that she was not suicidal and filed suit against the psychologist and the behavioral health center claiming that she was improperly committed based on a telephone conference between the psychologist and the woman's estranged husband who had informed the psychologist that the woman was suicidal. The woman further alleged that the psychologist had not performed the required evaluations and examinations prior to an involuntary commitment. The woman's claim against the behavioral health center relied on the center's failure to release the woman after determining that she did not pose a danger to herself or others and was not gravely disabled. Furthermore, the woman was forced by the center to take medication which was not appropriate for her condition. Had the psychologist performed an in-person evaluation, the woman argued, he would have determined that she was not suicidal. The claim was for personal injury, disability, physical pain and suffering, mental anguish, and loss of life enjoyment due to the defendants' alleged actions.

The physician responded that he had acted within the appropriate standard of care by conducting a thorough telephone consultation with the woman. The call between the physician and the woman had led the physician to believe that the woman was suffering from suicidal ideation and that she was indeed a threat to herself. In response, the woman stated that she had not spoken to the physician on this day and that the physician had failed to document the conversation on the Physicians Emergency Certificate which was required to be filed to effectuate the commitment.

The center also denied the woman's claim that it had breached the standard of care and alleged

that the woman did not have sufficient evidence to support such a claim. Summary judgment ultimately was awarded to the center, but the case was pursued against the psychologist. A jury verdict was returned in favor of the woman in the amount of $65,000: $15,000 for loss of enjoyment of life and $50,000 for mental anguish.

What this means to you: In this case the woman states that she had been involuntarily confined in to a behavioral health center for alleged suicide ideation. Involuntary treatment or confinement is treatment that is undertaken without the person's consent. In most cases, involuntary confinement refers to psychiatric treatment that is administered regardless of the patient's objection. Typically these are individuals who are deemed to be a danger to themselves or others. Most states allow some form of involuntary treatment for short periods of time under emergency conditions, but the criteria for confinement vary from state to state.

The justification for involuntary treatment is usually the potential for severe consequences if the patient is not treated. According to the background information, the woman had suffered a great loss during a time of increased stress. It appears that the initial contact with the psychologist was by the patient; however the subsequent contact was by the psychologist. It is unclear what prompted that conference call with the patient, but the information leads you to believe that the estranged husband recommended the conference call. Thereafter, the woman was involuntarily confined for nine days for suicide ideation.

The woman states that the psychologist did not perform the required evaluation and examination prior to the confinement. According to the State of Louisiana, Human Services Law, a mentally ill person may be admitted to a treatment facility for observation, diagnosis, and treatment not to exceed 15 days under an emergency certificate.

Any psychologist can execute an emergency certificate; however it requires an examination of the individual and documentation of such. Failure to conduct an examination prior to executing the certificate is considered negligence. The examination date cannot be more than 72 hours prior to the date on the certificate.

The examination should state objective findings relative to the mental condition of the individual that lead to the conclusion that the individual is a danger to herself. The certificate is valid for 72 hours and is delivered to the director of the treatment facility where the individual will be treated.

Upon admission to the treatment facility, the director notifies the coroner of the parish in which the treatment facility is located and advises him/her of the admission. The coroner or his/her deputy must independently examine the individual and execute the emergency certificate that is a necessary precondition to the individual's continued confinement.

In this case, the background information suggests that this process was not followed. In any treatment situation be it physical or mental illness, a face-to-face assessment and examination is necessary to appropriately diagnose and treat the individual. A telephone consultation can certainly provide some basic information, but a healthcare provider has a duty to examine the individual before coming to a conclusive diagnosis. At that point, the practitioner documents the findings and develops the treatment plan.

The Center for Medicare and Medicaid Services (CMS) and The Joint Commission (TJC) have specific standards or conditions for participation regarding patient assessments and reassessments. For psychiatric hospitals that use TJC for deemed status, each patient must receive a psychiatric evaluation within 60 hours of admission.

CMS states that psychiatric hospitals must protect and promote each patient's rights. Upon admission the patient should receive a thorough history and physical examination with all indicated laboratory examinations. This assessment is used to develop a treatment plan specific to the patient's needs.

It appears that this patient's rights were ignored by several individuals. According to the state laws for involuntary confinement, there was a requirement for an examination and signed certificate. Furthermore, the system is designed to have another practitioner examine the individual and sign a certificate, but it appears that the documentation of these examinations were not available.

There has been much controversy regarding involuntary confinements and possible misuse/abuse of such confinements. Critics have said that patients who have been confined and given psychiatric medications have suffered with disabilities following confinement. It appears that the patient's rights were not at the forefront in this case and that the standards of care for

involuntary confinement in this state were not followed. The key is to ensure proper procedures are followed and that the documentation supports the finding.

REFERENCE

District Court of Louisiana, Fifteenth Judicial Circuit, Parish of Lafayette, Case No. 99-4357. ■

Alleged: No treatment for ectopic pregnancy

Malpractice action questions causation

By **Radha V. Bachman**, Esq.
Buchanan, Ingersoll & Rooney, PC
Tampa, FL

Commentary provided by:
Barbara Reding, RN, LHCRM, PLNC
Central Florida Health Alliance
Leesburg
and **Leilani Kicklighter**, RN, ARM, MBA, CHSP, CPHRM, LHRM
The Kicklighter Group
Tamarac, FL

News: A pregnant woman experienced bleeding and cramps early on in her pregnancy. She visited her doctor, who confirmed that the woman was three weeks pregnant and diagnosed her with a probable spontaneous abortion. Prior to receiving an ultrasound to confirm the abortion, the woman experienced pain and presented to a local hospital. A pelvic ultrasound was ordered, and the reading radiologist noted "ectopic pregnancy is not ruled out. Please correlate clinically." The woman was seen by the hospital's chief obstetric resident, and the woman's symptoms were discussed with the supervising attending physician. Ectopic pregnancy again was listed as a possible diagnosis with a note that it was "clinically unlikely," and the woman was discharged. The woman continued experiencing severe abdominal pain. Eight days after being discharged, the woman again returned to the hospital emergency department. It was determined that her fallopian tube had ruptured as a result of an ectopic pregnancy. Subsequently, the woman instituted a medical malpractice action against the hospital and the supervising attending physician.

Background: A woman, who believed she was pregnant, began experiencing severe abdominal cramping and bleeding soon after completing a home pregnancy test. The woman made an appointment to see her primary care physician who determined that the woman was three weeks pregnant and had probably experienced a spontaneous abortion. The woman then was scheduled for a transvaginal ultrasound about one week later. Prior to receiving the ultrasound, the woman again began suffering from bleeding and went to the emergency department (ED) at a local hospital. A pelvic exam was conducted, blood was drawn, and a pelvic ultrasound was ordered. An OB consult was called, and no signs of active bleeding, blood, clots, or cervical dilation were noted. A pelvic ultrasound, however, indicated a possible ectopic pregnancy. An ectopic pregnancy occurs when a pregnancy implants outside the uterine cavity, typically in the fallopian tube. The radiologist who read the ultrasound determined that there were no signs of an intrauterine pregnancy and that ectopic pregnancy could not be ruled out.

The chief obstetrics resident at the hospital visited the woman and consulted with the supervising physician. The resident noted that the complex fluid in the cul de sac, an area between a female's rectum and back wall of the uterus, raised concerns of ectopic pregnancy. However, the resident said that such a diagnosis was "clinically unlikely." The woman was released with instructions to follow-up three days later. One day after her scheduled appointment, the woman came to the clinic and was seen by the resident. The resident confirmed that the woman was not pregnant and that there was no blood in the vaginal vault. However, he also noted that the woman should be placed on "strict ectopic pregnancy precautions" due to the fact that her beta levels had increased. The resident indicated that if the woman's beta levels continued to increase, she would be considered for an ultrasound and laparoscopy. The woman was released with instructions to return in a few days. That same day, the woman came back to the hospital again with severe cramping and told the nursing staff and the ED physician that she was "pregnant in her tube." Following a basic examination, she was diagnosed with muscle strain and discharged.

Four days after being discharged for the second time, the woman presented at another hospital's ED. The staff discovered that her fallopian tube had ruptured, and the woman underwent surgery

to remove the reproductive organs.

The woman filed suit against the hospital and the resident's supervising physician alleging negligent care. The woman's experts testified that had the ectopic pregnancy been treated during the woman's second visit to the hospital, she would not have suffered a ruptured tube. The plaintiff's experts also testified that administration of the drug methotrexate could have been used to treat the ectopic pregnancy. Methotrexate stops the growth of a developing embryo and is commonly used when a woman is suffering from an ectopic pregnancy.

Legal issues: The hospital and the physician defendant joined together to file a motion to dismiss, and they argued that the plaintiff was unable to show that the defendants' failures led to the woman's injuries. The trial court granted the motion and dismissed the case, and the plaintiff appealed.

On appeal, the court looked at whether there was a genuine issue of material fact with respect to the element of causation. A genuine issue of material fact exists when the record leaves open an issue upon which reasonable minds could differ. The appeal court found that, based on the expert testimony of four witnesses, the woman had presented sufficient evidence to create a genuine issue of fact with respect to whether the hospital and physicians' failure to diagnose and timely treat the ectopic pregnancy led to the rupture of her fallopian tube.

The hospital defendant attempted to argue before the appeals court that the woman's failure to return to the hospital for follow-up care as instructed by the resident was the sole cause of the rupture. The court rejected this argument and stated that issues of apportionment of liability and negligence are for a jury. The case was sent back to the trial court and will be continued.

What this means to you: In using as a guideline the definition of causation as "the departure from the standard of care must be the cause of the plaintiff's injury, and the injury must be foreseeable," this case evokes several thoughts from the risk management perspective. Based on the information provided, with no review of the actual records, it seems the care providers "struggled" with making a definitive diagnosis. A pelvic ultrasound (US) indicated a "possible ectopic pregnancy." That possibility alone would warrant additional and timely evaluation and action. According to the Mayo Clinic's online information for a health care consumer, the information provided indicates the "stakes are high" with an ectopic pregnancy where treatment might lead to loss of reproductive organs or infertility. Untreated, the "stakes are even higher" with potential for a ruptured fallopian tube that could result in life-threatening bleeding, according to the Mayo Clinic.

If an ectopic pregnancy was possible (as per pelvic ultrasound), the standard of care (SOC) would indicate the need for further evaluation and diagnosis because the injury, a fallopian tube rupture, was *foreseeable*. With SOC, injury alone is not proof that the defendant(s) deviated from the SOC.

It would be interesting to read the testimony of expert OB/GYN witnesses. Was the evaluation of the plaintiff timely and appropriate in light of the fact there was suspicion for an ectopic pregnancy? Did the attending/supervising physician come in to exam the patient? It would appear that there were more signs and symptoms to support ectopic pregnancy than support against it. If the evaluation and subsequent diagnostic studies were in line with the SOC, and there was either no departure from the SOC or a departure could be considered "reasonable," then the plaintiff would not be able to demonstrate proximate cause. It would seem the SOC must be thoroughly researched in this case before being able to determine causation. Was there truly a deviation from the SOC?

It appears that what happened in this unfortunate case was a failure to appropriately diagnose the ectopic pregnancy and implement timely clinical intervention. It seems a few of the involved physicians (resident and ED physician) had identified possible ectopic pregnancy and were pursuing potential remedial efforts while others (supervising physician) dismissed such a diagnosis without additional diagnostic studies. There is a wealth of information on the Internet regarding ectopic pregnancy, its signs and symptoms, complications, testing, treatment, etc. Given the severity of delayed treatment, the caregivers should have made ruling out ectopic pregnancy a primary goal. From the risk management perspective, this is one of those cases where, the organization's or facility's leaders should perform a thorough record review, obtain statements from physicians, and hold their breath. This case indeed is a most interesting one. The appellate court must have thought so as well.

REFERENCE

Michigan, Genesee Circuit Court; LC No. 08-087809-NH. ■