Healthcare RISK MANAGEMENT

The Trusted Source for Legal and Patient Safety Advice for More Than Three Decades

November 2013 | Vol. 35, No. 11 Pages 121-132

Drug testing after adverse events is a controversial idea

Some say it's time to test clinicians, but expect resistance

Mandatory drug and alcohol testing is routine for pilots and train conductors after a crash, so shouldn't healthcare providers also test physicians after an adverse event? This idea is being floated by some notable names in the industry who say that even if the idea seems radical, it could improve patient safety.

Post-event testing should be seen as part of an organization's overall approach to dealing with impaired physicians, says **Peter Pronovost**, MD, PhD, FCCM, a practicing anesthesiologist, critical care physician, professor, senior vice president of Johns Hopkins Medicine in Baltimore, MD, and senior vice president and director of the Armstrong Institute for Patient Safety and Quality at Johns Hopkins.

"There seems to be a problem, as with in all of society, with physicians who are impaired, and we need to have an effective strategy for both supporting those physicians and protecting patients," he says. "Using routine surveillance in conjunction with testing after adverse events would be an effective strategy."

> *"... we need to have an effective strategy for both supporting those physicians and protecting patients."*

Pronovost and colleagues proposed post-event testing, along with pre-employment and routine drug testing, in a commentary published online recently in *The Journal of the American Medical Association*. *(See the story on p. 123 for more on that commentary.)*

Those who support the idea concede that there is no research showing a link between adverse events and drug or alcohol impairment. Pronovost argues that "given the prevalence of substance abuse in healthcare and the number of adverse events, it would be hard to imagine there is not an overlap somewhere in those two circles."

Another proponent of the idea is the

INSIDE

AHC Media

www.ahcmedia.com

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

highly regarded medical ethicist **Arthur Caplan**, PhD, director of the Division of Medical Ethics at New York University's NYU Langone Medical Center in New York City. He says testing is needed partly because no one knows if there is a causal connection between alcohol and drug use and adverse events.

"In other industries like transportation, they have enough evidence to know that drug and alcohol use plays a role in accidents, and I don't see any reason to think that would be any different for doctors and nurses," Caplan says. "We know that the availability of drugs makes abuse possible for many healthcare professionals, and a particular risk in some specialties. So it's not like we don't know that doctors sometimes abuse drugs."

Near misses also should prompt drug and alcohol testing, Caplan says. Physicians and other clinicians certainly will resist the idea of mandatory testing after an adverse event, Caplan says, but he sees nothing about the healthcare industry that should exempt it from the same standards used in other workplaces.

"A lot of people think we're making an accusation when you test, but it's really an inquiry," he says. "It may go better in the context of testing after an adverse event than if you implemented routine random testing, but any kind of drug and alcohol testing has a stigma. Doctors want to be trusted, but I go by the old Cold War adage that you trust, but verify."

It is believed that no healthcare providers currently require drug and alcohol testing after adverse events, but interest in post-event testing has grown since Pronovost and his colleagues first proposed the idea. Leaders at his own institution, Johns Hopkins, and other facilities have contacted him to discuss the logistics of setting up such a program.

"We are in discussion phases here, and several other places are considering it also. We're hearing from a lot of risk managers who say this just makes sense," he says. "Even routine testing is not done in healthcare right now, and that might be more easily implemented and would pick up a lot of problems even if you don't do testing after adverse events."

False positives could be devastating to a physician or nurse's career, but Pronovost says testing has become so reliable that false positives virtually can be eliminated by using more advanced techniques

Executive Summary

Prominent healthcare leaders are calling for providers to start mandatory drug and alcohol testing after adverse events, but others say there is not enough evidence that such a policy is necessary. Proponents and critics agree that introducing such a policy would be difficult.

- ✦ A testing policy would face significant legal hurdles.
- ✦ Other industries already require testing after accidents.
- ✦ Peer review programs might have to be modified to allow testing.

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

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

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

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

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

Healthcare Risk Management® is intended for risk managers, health system administrators, and health care legal counsel. Opinions expressed are not necessarily those of this publication. Mention of products or services does not constitute endorsement. Clinical, legal, tax, and other comments are offered for general guidance only; professional counsel should be sought for specific situations.

Executive Editor: **Joy Daughtery Dickinson** (404) 262-5410 (joy.dickinson@ahcmedia.com). Production Editor: **Kristen Ramsey.** Interim Editorial Director: **Lee Landenberger.**

SUBSCRIBER INFORMATION

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

Subscription rates: U.S.A., 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.)

on samples that initially indicate impairment. Defining an adverse event is another challenge, but Pronovost says providers could start with preventable deaths or sentinel events. Those are clearly adverse events and could be the first threshold for triggering post-event testing. After working out the kinks with that level of testing, a provider might lower the threshold to include other adverse events, he suggests.

Implementing a testing program will require extensive education about the purpose, Caplan says. Simply announcing that you will begin testing after adverse events will result in huge pushback, he says. There also can be legal limitations to such testing and potential liability for the hospital. *(See the story on p. 124 for more on the legal issues.)*

"Given the concern about quality of care and patient safety in healthcare institutions, I can't imagine that we wouldn't want to push in this direction," Caplan says. "I see it as part of a quality control push rather than a punitive measure or trying to respond to a drug epidemic."

Another prominent ethicist takes a dim view of the idea. **John Banja**, PhD, medical ethicist at the Center for Ethics at Emory University in Atlanta, says he opposes drug and alcohol testing after adverse events because there is no evidence to suggest impairment is linked to errors and bad outcomes.

"I don't like the proposal. It unfairly singles out doctors for drug and alcohol testing without any evidence there is a causal relationship," Banja says. "The literature clearly shows that when you have one of these nasty sentinel events go down at your hospital, it is almost always the result of multiple people making multiple mistakes."

"People simply make human mistakes, and largely because they are attempting to satisfy productivity goals."

Given that fact, a testing program should include dozens of people who were involved with the case, Banja says. That system would prove impractical and costly, he says. If it is done at all, the testing also should be extended to near misses in which errors were made but the patient was not harmed, he says, which would further expand the program.

"You can imagine how many drug tests you would be doing in a hospital every day," Banja says. "Think of a 500-bed hospital and how many errors and near misses occur, and how many people are involved in each of those. You'd be testing everyone all the time."

Banja also suspects that the testing program would find very few cases in which the adverse events could be blamed on an impaired physician or other clinician.

"People simply make human mistakes, and largely because they are attempting to satisfy productivity goals," Banja says. "A more productive strategy would be to encourage people to speak up when they see someone acting in an unsafe way. We know that people often will see something that makes them uncomfortable, but they don't speak up or they just keep it under the radar and talk among themselves."

SOURCES:

- **John Banja**, PhD, Medical Ethicist, Center for Ethics, Emory University, Atlanta. Telephone: (404) 712-4804. E-mail: jbanja@emory.edu.
- **Arthur Caplan**, PhD, Director of the Division of Medical Ethics, New York University NYU Langone Medical Center, New York City. Telephone: (646) 501-2739. Email: arthur.caplan@nyumc.org.
- **Peter Pronovost**, MD, PhD, FCCM, Senior Vice President, Johns Hopkins Medicine, Baltimore, MD. Telephone: (410) 502-3231. Email: ppronovo@jhmi.edu. ✦

Testing needed at least after sentinel events, doctors say

Hospitals should require mandatory alcohol-drug testing for clinicians involved with unexpected deaths or sentinel events and possibly more often than that, according to a commentary published online recently in *The Journal of the American Medical Association* (*JAMA*) by **Peter Pronovost**, MD, PhD, FCCM, a practicing anesthesiologist, critical care physician, professor, senior vice president of Johns Hopkins Medicine in Baltimore, MD, and senior vice president and director of the Armstrong Institute for Patient Safety and Quality at Johns Hopkins, and colleagues.

The authors recommend in their commentary that hospitals take several steps as a model to address what they consider an overlooked patient safety issue. They are:

- mandatory physical examination, drug testing, or both, before a medical staff appointment to a hospital. This step already occurs in some hospitals and has been successful in other industries;
- a program of random alcohol/drug testing;
- a policy for routine drug/alcohol testing for all physicians

involved with an adverse event leading to patient death;

• establishment of testing standards by a national hospital regulatory or accrediting body.

The steps could be limited to hospitals and their affiliated physicians at this time, because hospitals have the infrastructure to conduct adverse event analysis and drug testing, note the authors. Hospitals also have the governing bylaws to guide physician conduct, and The Joint Commission can help with establishing standards, the authors add.

In cases in which a physician is found to be impaired, a hospital could "suspend or revoke privileges and, in some cases, report this to the state licensing board," the authors write. Impaired physicians would undergo treatment and routine monitoring as a condition for continued licensure and hospital privileges.

The full commentary is available online at http://tinyurl.com/kn65jmp. A *JAMA* subscription is required. ✦

Many legal issues complicate drug and alcohol testing

Drug and alcohol testing after adverse events will come with a ton of potential legal problems. If you plan to implement such a program, think carefully about how you can construct it to reduce your liability risks and reduce friction with the medical staff.

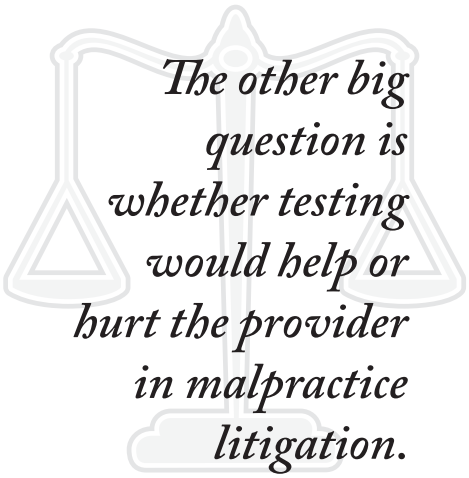
It is possible to write physician bylaws to require drug and alcohol testing after an adverse event, but there will be many complicating factors that can threaten the effectiveness of any testing and expose the hospital to liability, says **Michael R. Callahan**, JD, a partner with the law firm of Katten Muchin Rosenman in Chicago.

"The only way to implement this is through the medical bylaws. If it is not in the bylaws, your physicians are going to say that they don't have to comply, and they will be right," Callahan says. "Your first real hurdle will be getting this requirement into the bylaws."

Another challenge will be defining what constitutes an adverse event and triggers the testing requirement. Only a strict, specific definition would have any chance of being entered into the bylaws and surviving a legal challenge, Callahan says.

"If you tried to say you're going to test after all adverse events, and you don't specify what it means and limit it to only the most justifiable conditions, you will have a rebellion among your medical staff," he says. "You have more leverage with your employed physicians, because you can impose more employment qualifications on them and set the bar higher."

Some attorneys see merit in the idea. Testing after an adverse event should be part of the post-event analysis, says **Kathryn R. Coburn**, JD, an attorney with the law firm of Kobrick and Wu in Los Angeles.



The other big question is whether testing would help or hurt the provider in malpractice litigation.

She advises drawing up a contract in which the physician agrees to such testing before being hired or credentialed by the hospital, with carefully defined terms. The policy must be applied uniformly, and adhere to the triggers outlined in the contract.

"It also is important to be aware of the Americans with Disabilities Act [ADA]," Coburn says. "It does not protect current drug and alcohol users, but the definition of 'current' is a little fuzzy. You want to be very careful that people with a known problem are treated no differently. They cannot be treated more often or under different parameters."

The other big question is whether testing would help or hurt the provider in malpractice litigation, says **Michael Thompson**, JD, an attorney with the law firm of Reed Smith in Philadelphia. The results of the testing almost certainly would be available to the plaintiff, he says. State legislation could protect the test results as part of peer review, but there is no such protection now.

"If a hospital goes with this policy, you have to expect that those test results are going to be discoverable by the plaintiff," Thompson says. "And if you have a case where you have test results showing the doctor was impaired when he or she made a serious error and harmed the patient, that's going to be a very difficult case to defend."

SOURCES:

• Michael R. Callahan, JD, Partner, Katten Muchin Rosenman, Chicago. Telephone: (312) 902-5634. Email: michael.callahan@kattenlaw.com.

• Kathryn R. Coburn, JD, Kobrick and Wu, Los Angeles. Telephone: (424) 238-4501.

• Michael Thompson, JD, Reed Smith, Philadelphia, PA. Telephone: (215) 851-8871. Email: mthompson@reedsmith.com. ✦

Fraud self-disclosure requires careful strategy

Nobody wants to run afoul of the Stark law or other fraud prevention regulations, but it happens. You analyze a complex interaction between healthcare providers and realize that you have violated the law, perhaps in some highly technical manner. What now?

Self-disclosure might be your best option. Go ahead and confess to your error and hope the government regulators go easy on you. But even if that is the best path, you must tread carefully, cautions **Jeffrey E. Rogers**, JD, a partner with the law firm of McGuire Woods in Chicago. The first step is to be certain you actually have violated the law before you invite regulators inside. *(See the story on p. 126 for more on ensuring you have a violation to report.)*

The Department of Health and Human Services (HHS) Office of the Inspector General (OIG) and Congress have altered the Provider Self-Disclosure Protocol to make it easier and more beneficial, Rogers notes, but at the same time they broadened the OIG's ability to punish those who do not report. One change was especially significant for providers: In the updated Provider Self-Disclosure Protocol, OIG states that self-reporting will presumptively indicate an effective compliance program and that no corporate integrity agreement (CIA) is needed.

Complying with a CIA can be onerous for a healthcare provider, so the ability to avoid one with self-disclosure is a major incentive, Rogers says. OIG also announced that it will impose penalties of only 1.5 times the damages in self-disclosure cases, which is much less than the amounts sometimes sought by the government.

OIG also created an online submission process for self-disclosure in hopes of streamlining the disclosure process, Rogers notes. The changes already are having the desired effect: HHS officials have said they expect to receive about 100 self-disclosures of Stark violations in 2013. There have been almost 300 self-disclosures since the 2010 passage of the Affordable Care Act, which also contained incentives for self-disclosure. However, the OIG is way behind in resolving those cases.

With the government continuing to aggressively prosecute fraud in healthcare, self-disclosing can look increasingly attractive, Rogers says. Prosecution can result in treble damages under the False Claims Act, civil monetary penalties, and even criminal prosecution. However, self-disclosure is not without its own risks.

One potential risk relates to how the OIG shortened the time period for completion of the disclosing party's investigation from 90 days following acceptance into the program to 90 days following initial submission.

"That change apparently was intended to be a benefit for healthcare providers, but it can cause problems," Rogers explains. "Changing the term from acceptance to initial submission means a shorter timeframe, and that could force the disclosing party to rush through an investigation that really needs more time to be thorough and accurate."

In addition, risk managers should be concerned that the disclosure could be made available to private litigants, including existing or potential *qui tam* relators. The recent update to the protocol requires that the healthcare provider detail what civil and criminal laws were violated, which potentially provides a more detailed guide for plaintiffs' attorneys than they ever had so easily available, Rogers says.

The OIG has clearly stated that it will coordinate with the Department of Justice in the resolution of self-disclosure cases, Rogers notes. The worst part is that the OIG made clear it will defer to the DOJ if the two agencies disagree on how to resolve a case.

Still, Rogers says self-disclosure is almost always the best choice. Trying to lay low and hope the government doesn't discover your violation is an increasingly big risk, he says.

"You've got more whistleblowers than ever before and more *qui tam* cases than ever before. We're also seeing more competitors complaining because your arrangement might be driving them out of business," Rogers says. "It used to be that if the government didn't intervene, the relator just went away. But now the *qui tam* bar is so much more sophisticated and aggressive that they will be willing to run with the thing even if the government doesn't."

The government also is conducting more audits that can detect these violations, and self-disclosing could fend off an audit that might uncover additional problems, Rogers notes.

That assessment is seconded by **Karl A. Thallner Jr.**, JD, a partner with the law firm of Reed Smith in Philadelphia. He says that once you determine a violation has occurred, a first priority should be determining the most painless way to resolve it.

Executive Summary

The government has changed rules regarding self-disclosure after a healthcare provider discovers it has violated the law. Disclosing your violation is now easier and more beneficial, but the government has more ability to punish those who do not report.

- ✦ The number of self-disclosures has risen sharply.
- ✦ The Office of Inspector General (OIG) is far behind in resolving the disclosures.
- ✦ Any plan to self-disclose must be carefully considered.

"Was this a Stark-only problem, a technical violation like an agreement expired or was it signed after the relationship began?" he says. "Or was there a reason to believe this problem is more serious, that someone was intending to contend a benefit on the physician to induce referrals?"

A technical violation can be easier to address than the other, Thallner says. Both might have to be disclosed, but a technical violation can be reported in much more straightforward way with an explanation and evidence of repayment, if necessary. A scheme to induce referrals is far more serious. *(See the story below for more on how to disclose violations.)*

"The days of sweeping these violations under the rug are over," Rogers says. "The other advantage to self-reporting is that you have the opportunity to paint the picture of the situation in the manner most favorable to yourself. You get to frame it, narrow the issues, phrase things certain ways so that it doesn't look like the worst thing the government's ever seen."

SOURCE:

• **Jeffrey E. Rogers**, JD, Partner, McGuire Woods, Chicago. Telephone: (312) 750-8686. Email: jrogers@mcguirewoods.com. ✦

Slow down and be sure you have violated law

If you think your helathcare organization has violated the Stark law or other fraud prevention measures, the very thought of treble damages (triple the actual monetary loss) from a government prosecution could prompt you to self-disclose as soon as possible in hopes of a lesser punishment. However, you should wait before you do anything, legal experts advise.

Before you do anything hasty, make absolutely sure that you have a violation to report, advises **Karl A. Thallner Jr.**, JD, a partner with the law firm of Reed Smith in Philadelphia. He has seen healthcare providers come to him with what they thought were violations of the law that should be self-disclosed, but on further investigation they determined otherwise.

"Stark is extraordinarily complicated, and people sometimes make assumptions about the existence of a violation," Thallner says. "If you parse through it all in a technical way, you can find that there may be an argument, if not some certainty, that there was no violation."

Thallner recalls one instance in which a hospital leased office space to a nephrologist. The hospital inadvertently failed to renew the lease agreement. That put them out of compliance with the office rental exception under Stark, but on further review the attorney realized that the dialysis services ordered by the hospital were furnished by a dialysis center and those services are not designated health services under the Stark law.

"People were assuming we had a violation with the lease exception, and on that count alone it seemed something to disclose," Thallner says. "But because the services were not covered under Stark, there was in fact no problem. It's worth spending some real time to figure out if there is a legitimate basis for concluding there was no violation."

If double- and triple-checking yields the same conclusion that you have violated the law, Thallner says self-disclosure usually is going to be the way to go.

"Doing nothing is usually the worst thing to do," he says.

SOURCE:

• **Karl A. Thallner Jr.**, JD, Partner, Reed Smith in Philadelphia. Telephone: (215) 851-8171. Email: kthallner@reedsmith.com. ✦

Repayment can be part of disclosure plan

If you repay within 60 days, it could help your case

Some violations of Stark and other laws can be resolved largely through repayment of the money involved, explains **Karl A. Thallner Jr.,** JD, a partner with the law firm of Reed Smith in Philadelphia. You still might need to disclose the violation, but the government is likely to go easier on you if already have repaid the money.

"If there's a Stark noncompliant arrangement with an anesthesiologist, and the anesthesiologist orders some services that the hospital provides but not much, then one approach would be to just make a repayment for the Medicare-reimbursed hospital services that derived from the referral," Thallner says. "If you do that within 60 days of when it is identified, you've done what they want, and I think you're going to be in good enough shape."

If the repayment is a clean, clear solution to an oversight, self-disclosure might not be necessary, Thallner says.

A bigger problem is a Stark-noncompliant significant referral source, Thallner says. When the value of the services referred is so high that immediate repayment is impractical, then you will have to go through the self-referral protocol.

"If you're exposing yourself to the government through a disclosure, you have to be truthful and open in a way that doesn't make the government suspect something serious and untoward is going on," Thallner says. "You will have to spend a lot of time determining how you want to tell the story so that it is truthful but positions the violation as an isolated problem and you have determined how to prevent a recurrence." ✦

Telemedicine brings more risk with more use

Telemedicine has been the new frontier of caregiving for years, but it finally is becoming a reality at many healthcare facilities. That change means that the liability risks discussed in theory up to this point are becoming real, and risk managers must act quickly to address them.

Whereas the use of telemedicine in the early years was mainly the purview of leading edge physicians who either devised their own long-distance connections or worked with academic researchers, hospitals are now being approached by companies offering to provide telemedicine capabilities. That change magnifies some of the potential liability risk, says **Mark Kadzielski**, JD, an attorney with the law firm of Pepper Hamilton in Los Angeles.

"A risk manager should be very, very aware of the issues when someone at your facility says they are going to contract for telemedicine services," he says. "There will need to be a written agreement for telemedicine services, which needs to be looked at carefully because of the myriad legal issues involved."

Telemedicine is defined by the Centers for Medicare and Medicaid Services (CMS) as "the provision of clinical services to patients by practitioners from a distance via electronic communications," and by the American Telemedicine Association (ATA) as "the delivery of any healthcare service or transmission of wellness information using telecommunications technology."

The technology will be employed more in coming years as a way to compensate for the increased patient load and the lack of physicians, Kadzielski predicts. "Given the expansion of access under Obamacare, telemedicine is a natural fit so that people in remote areas and busy urban areas without enough doctors can be seen," he says. "It can be a wonderful component of care if used properly."

There are many significant unaddressed legal issues that risk managers must face to ensure that their telemedicine services are compliant with federal and state requirements. One of the first concerns is reimbursement. Medicare reimbursement for telemedicine services is limited, but CMS has indicated that it might expand the payment possibilities. *(See the story on p. 128 for more on the CMS position.)* Medicaid reimbursement varies from state to state, though at least some type of reimbursement is offered in the majority of states, Kadzielski explains.

Due to the varied reimbursement climate, hospitals, healthcare organizations, and healthcare systems should do the following:

- Be aware of the federal and state reimbursement laws and restrictions that might affect their billing practices.
- Know what telemedicine services will and will not be reimbursed.
- Know how to bill for certain telemedicine services.
- Only submit compliant claims to avoid liability for fraud and abuse and false claims.

"When you're offered a contract and people say don't worry because you'll split the money, that raises all sorts of concerns about fraud and abuse," Kadzielski says. "And of course, if what you're splitting turns out to be zero, that's going to cause a contractual dispute faster than you can imagine." *(See the story on p. 128 for more on the potential liability associated with telemedicine.)*

There is very little case law regarding telemedicine, and most of what exists involves criminal charges related to prescribing medicine across state lines, says **Paul Hildebrand**, MD, associate director of the patient safety organization TeamHealth in Knoxville, TN, and regional director of quality with the San Franciscan Health System in Tacoma, WA. Though he agrees there are many potential risks, he sees the possibility of telemedicine actually reducing liability in some ways.

"The overall risk could be diminished by telemedicine because you're able to provide a service that you might not otherwise have been able to provide," Hildebrand says. "If the patient can get the care they need, regardless of where they are located, that can be a positive aspect in terms of patient care and liability."

Hildebrand recalls one physician who was making use of email and electronic health records to communicate with patients, to the extent that his malpractice insurer decided to audit him, because staff there feared that the remote consultations were jeopardizing patient care and creating liability risks. After looking at his email use, the malpractice insurer reduced his premium.

"They found that his use of telemedicine improved his relationship with patients, rather than leaving them to grow angry over long waits for an appointment," he says.

Hildebrand and Kadzielski urge risk managers to address the risk management issues related to telemedicine immediately, even if the technology is

Executive Summary

Healthcare providers are using telemedicine more than in past years. Risk managers should address known liability risks as the use of this technology becomes more commonplace.

✦ Fraud and abuse charges are possible if telemedicine reimbursement is not addressed properly.

✦ Physician credentialing and privileging must take into account the unique aspects of telemedicine.

✦ Medical staff bylaws should include telemedicine use.

not yet employed widely. If it is not yet a significant part of your organization's caregiving, it soon will be, they say.

"You have to worry about the risk now. You can't kick the can down the road," Kadzielski says. "Given the exponential expansion of telemedicine services, the time to be concerned about the risk is now, not tomorrow."

SOURCES:

• Paul Hildebrand, MD, Associate Director, of Patient Safety Organization, TeamHealth, Knoxville, TN. Telephone: (235) 549-6525. Email: tom_hildebrand@teamhealth.com.

• Mark Kadzielski, JD, Attorney, Pepper Hamilton, Los Angeles. Telephone: (213) 928-9820. Email: kadzielskim@pepperlaw.com. ✦

CMS hints at more telemed payment

The Centers for Medicare and Medicaid Services (CMS) is considering paying primary care physicians for chronic care management services without an in-person visit, and also for telehealth services. Keep a close tab on how this proposal fares as you work to avoid fraud and abuse issues with telemedicine.

CMS proposed the improved payment in the Medicare Physician Fee Schedule for 2014 and suggested a change that would start in 2015. Under the CMS proposal, patients would need to have an annual, in-person wellness visit and consent to a doctor's management plan for a year. To make telehealth reimbursement possible, the proposal redefines the definition of "rural" to avoid disruption of services if an area's geographic designation is changed. CMS said in the proposal that it is looking for evidence that "the service furnished by telehealth to a Medicare beneficiary improves the diagnosis or treatment of an illness or injury" or that it improves patient functioning.

CMS would reimburse for telehealth only if it is provided by one of eight kinds of healthcare professionals. Additionally, only certain kinds of codes are eligible, mostly involving screening and mental healthcare. ✦

Credentialing, peer review pose problems

There are many potential liability risks that come with the growing use of telemedicine. **Mark Kadzielski**, JD, an attorney with the law firm of Pepper Hamilton in Los Angeles, offers this summary:

• **Physician credentialing and privileging:** In July 2011, the Centers for Medicare and Medicaid Services (CMS) enacted its final rule on telemedicine credentialing and privileging and gave healthcare facilities and practitioners more flexibility to accomplish credentialing and privileging of practitioners by doing away with the need for an independent review. CMS' final rule provided processes by which hospitals may rely on the credentialing and privileging decisions of distant-site hospitals or the information provided by other telemedicine entities when making decisions on privileges for practitioners who provide telemedicine services, as long as certain conditions, such as a written agreement between the hospital and distant site, are met.

Soon after, The Joint Commission revised its standards and telemedicine requirements to align with CMS' requirements. Although many states have followed suit, hospitals, healthcare organizations, and healthcare systems must ensure that their credentialing and privileging processes are compliant with federal and state laws as well as the requirements of accreditation bodies to mitigate possible negligent credentialing claims and other risks.

When entering into written agreements with telemedicine entities that claim to credential and privilege their practitioners, hospitals, healthcare organizations, and healthcare systems must determine that any written agreement they receive from a telemedicine entity has been appropriately updated to reflect current legal requirements, clearly establish specific responsibilities of distant-site hospitals and other telemedicine entities, and ensure that written agreements include adequate representations and warranties with regard to the quality of services provided by the distant site and any entity with which the distant site subcontracts. Even then, there still will be risks.

"The risk management concern is that lots of people are pushing telemedicine contracts at you, offering to have doctors you don't know, whose credentials you don't know, practice telemedicine on your patients in your facility," Kadzielski says. "There is great risk when you have telemedicine providers rendering services to your patients and you have not verified that the doctor is up to par. You're relying on someone else's assessment."

• **Medical staff bylaws:** Under CMS' final rule, when a hospital intends to credential and privilege distant-site practitioners for telemedicine services, the hospital's medical staff bylaws must include criteria for determining the privileges to be granted to such practitioners and a procedure for applying the criteria

to those practitioners. Hospitals that credential and privilege distant-site practitioners based on information received from a distant site must review and revise their medical staff bylaws and credentialing and privileging policies to include specific criteria that outline how privileges to distant-site practitioners will be granted in accordance with a written agreement with a distant site.

"Revisions should also be made to address what category of the medical staff certain distant-site practitioners will join, the level of involvement distant-site practitioners may have in medical staff committees, and what procedural rights distant-site practitioners may have," Kadzielski says.

• Physician peer review: As more hospitals, healthcare organizations, and healthcare systems rely on the decisions made by distant-site hospitals or the information provided by other telemedicine entities when making credentialing and privileging decisions, written agreements with the distant site detailing how peer review and internal review information will be shared between the hospital and distant site are required. Hospitals, healthcare organizations, healthcare systems, and telemedicine entities must develop procedures and policies for sharing such information to ensure that the privacy of physician peer review and patient information is appropriately protected while information needed to make accurate credentialing and privileging decisions is regularly shared.

Because information is being shared between two distinct entities, it is essential that any procedure or policy complies with federal privacy laws, including the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH), and is disclosed in a manner that preserves all peer review privileges under state law.

There is great risk when you have telemedicine providers rendering services ... and you have not verified that the doctor is up to par.

• **Patient privacy:** Although "HIPAA" and "HIPAA compliant" have become buzzwords among telemedicine entities and vendors, prior to relying on any telemedicine technology to collect and transfer patients' protected health information (PHI), hospitals, healthcare organizations, and healthcare systems should ensure that they have the appropriate secure communication channels in place; have implemented entity- and technology-specific business associate and other confidentiality and privacy agreements, as applicable; have created policies and educated all administrators, employees, and medical staff members regarding the appropriate use of telemedicine technologies; and clearly understand how and what patient information is being collected, communicated, and stored.

Where practitioners provide healthcare services through telemedicine entities, such as tele-radiology, tele-neurology, tele-psychiatry, and tele-dermatology services, written agreements should identify what patient health information may be shared and how telemedicine practitioners will use or maintain patient health records for patient care and healthcare liability purposes. ✦

Incident reports don't tell whole story

Several studies have shown that hospitalized patients still have unacceptably high rates of harm and injury due in part to limited access for quality staff to obtain primary care data from electronic medical records. As a result, hospital incident reports do not capture most harm that occurs in hospitals, according to a study published in the *Journal for Healthcare Quality*.

The study showed that using administrative data, such as discharge abstracts, can gauge the quality of care and identify opportunities for improvement. The purpose of the study was to develop a new global measure of harm, called "whole patient measure of safety," that uses administrative claims data to measure the incidence of 14 "highly undesirable events" (HUEs).

The goal is to determine the probability for a patient to complete a hospital stay without any HUEs and the central measurement question is, "What proportion of hospitalized patients experience at least one HUE during their episode of care?" Data from 6.5 million discharge abstracts in 161 hospitals from July 1, 2008, to June 30, 2010, were studied.

Results of the analysis showed that the percent of hospitalizations with at least one HUE varied greatly among hospitals (13.32% to 1.99%) with a mean of 7.74%. Hospital-acquired infections (HAIs) were the most common HUE across all facilities, and blood incompatibility was the least common. HAIs usually result in readmission within 72 hours, and half of the HAIs identified occurred with other HUEs.

The study concluded that the

new whole patient measure of safety provides a global assessment of what happens to hospitalized patients as they move through the care system. It assesses the entire care process and can augment patient assessment metrics for specific diseases and procedures. The measures can be used to help hospitals interested in understanding where the most egregious safety deficiencies exist by examining patients with multiple HUEs.

Also, since hospital-acquired conditions are not being reimbursed by payers, administrative data can be a valuable resource to help gauge potential liability and risk and identify opportunities for improvement.

An abstract of the study is available online at http://tinyurl.com/ohot46g. ✦

Specific patient safety steps urged for hospitals

The head of The Joint Commission is urging hospitals to make substantial changes to achieve the ultimate goal of zero patient harm by adapting lessons from high-risk industries.

President and CEO **Mark R. Chassin**, MD, FACP, MPP, MPH, called for the safety improvements in an article along with **Jerod M. Loeb**, PhD, executive vice president for healthcare quality evaluation at TJC. The article was published in *The Milbank Quarterly* and is available online at http://tinyurl.com/kq34mgt.

Chassin and Loeb report that too many hospitals and healthcare leaders experience serious safety failures as routine and inevitable parts of daily work. To prevent the harm that results from these failures, which affect millions of Americans each year, the article specifies a framework for major changes involving leadership, safety culture, and robust process improvement. This framework is designed to help hospitals make progress toward high reliability, which is the achievement of extremely high levels of safety that are maintained over long periods of time, such as safety comparable to that demonstrated by the commercial air travel, nuclear power, and amusement park industries.

TJC tested the high-reliability framework, detailed in the article, at seven U.S. hospitals, as well as through face-to-face meetings and testing with healthcare leaders. In the article, Chassin and Loeb outline the 14 components of the high-reliability framework and contend that:

• Hospital leaders must commit to the ultimate goal of high reliability or zero patient harm rather than viewing it as unrealistic. The leadership section of the framework identifies specific roles for the board of trustees, the chief executive officer, and all senior management (including nursing leaders), the engagement of physicians, the hospital quality strategy, its use of data on measures of quality, and the use of information technology to support quality and safety improvement.

Hospitals must create a culture of safety that emphasizes trust, reporting, and improvement.

• Hospitals must create a culture of safety that emphasizes trust, reporting, and improvement. This means hospitals must put a stop to the intimidation and blame that drive safety concerns underground and instead emphasize accountability and the early identification of unsafe practices and conditions. A systematic approach that includes safety culture measurement is crucial.

• Hospitals need new process improvement tools and methods, in the form of a combination of Six Sigma, Lean, and change management (known together as Robust Process Improvement), to make far greater progress toward eliminating patient harm. Government regulation is unlikely to drive high reliability, but identifying and eliminating mandates that do not directly contribute to or distract from quality challenges is necessary. Well-crafted programs that require public reporting of reliable and valid quality measures also are recommended.

"Although no hospital has been able to achieve high reliability, there are some very practical changes that can be made to improve safety and quality," Chassin wrote in the article. "The time is now to start taking the steps needed to get from where we are today to where we want to be."

The article by Chassin and Loeb notes that the primary drive for change must come from within the healthcare industry and from hospitals themselves. TJC is developing an assessment tool that will allow hospitals to measure their current state of maturity across each of the high-reliability framework's 14 components. In addition, TJC is field testing tools that can be used to work toward high reliability. ✦

COMING IN FUTURE MONTHS

- ✦ Accurate incident reports
- ✦ Career advice for risk managers
- ✦ Ideas for creative fall prevention
- ✦ Conduct a more effective in-service

CNE OBJECTIVES

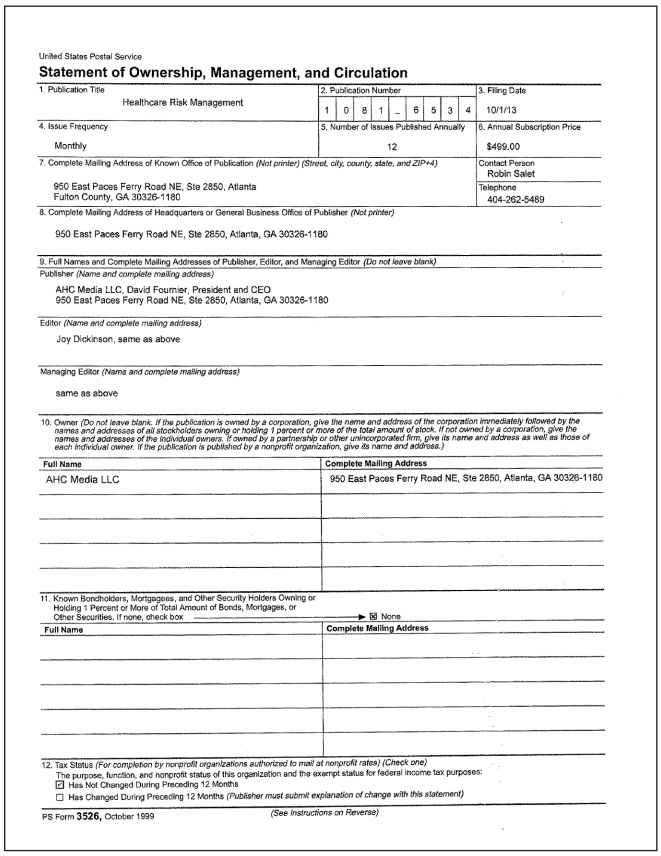
Upon completion of this educational activity, participants should be able to:

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

CNE INSTRUCTIONS

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

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



United States Postal Service

Statement of Ownership, Management, and Circulation

1. Publication Title	2. Publication Number	3. Filing Date
Healthcare Risk Management	1 0 8 1 _ 6 5 3 4	10/1/13
4. Issue Frequency	5. Number of Issues Published Annually	6. Annual Subscription Price
Monthly	12	$499.00

7. Complete Mailing Address of Known Office of Publication *(Not printer) (Street, city, county, state, and ZIP+4)*
950 East Paces Ferry Road NE, Ste 2850, Atlanta
Fulton County, GA 30326-1180
Contact Person: Robin Saliet
Telephone: 404-262-5489

8. Complete Mailing Address of Headquarters or General Business Office of Publisher *(Not printer)*
950 East Paces Ferry Road NE, Ste 2850, Atlanta, GA 30326-1180

9. Full Names and Complete Mailing Addresses of Publisher, Editor, and Managing Editor *(Do not leave blank)*
Publisher *(Name and complete mailing address)*
AHC Media LLC, David Fournier, President and CEO
950 East Paces Ferry Road NE, Ste 2850, Atlanta, GA 30326-1180

Editor *(Name and complete mailing address)*
Joy Dickinson, same as above

Managing Editor *(Name and complete mailing address)*
same as above

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

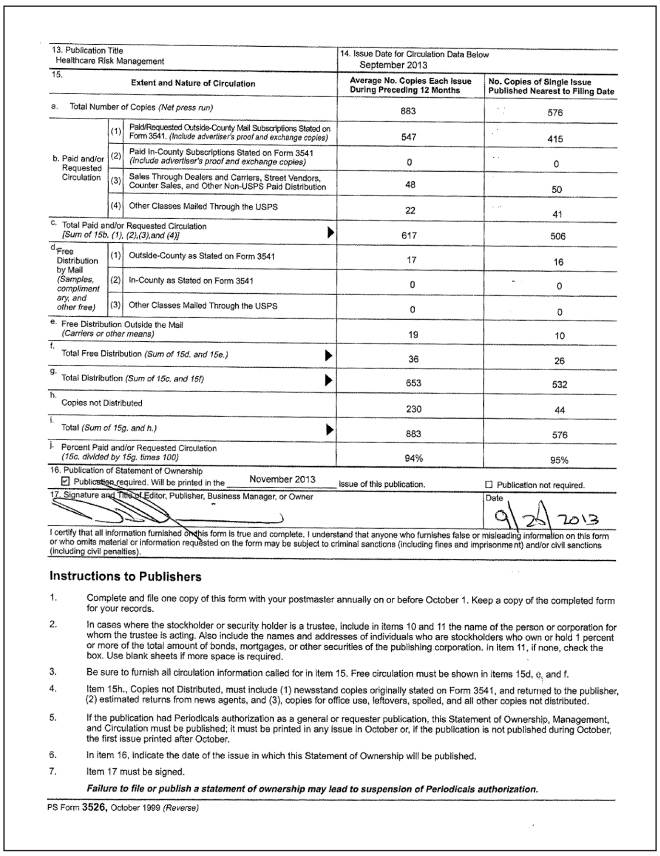
Full Name	Complete Mailing Address
AHC Media LLC	950 East Paces Ferry Road NE, Ste 2850, Atlanta, GA 30326-1180

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

Full Name	Complete Mailing Address

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

PS Form **3526,** October 1999 *(See Instructions on Reverse)*



13. Publication Title: Healthcare Risk Management	14. Issue Date for Circulation Data Below: September 2013	
15. Extent and Nature of Circulation	Average No. Copies Each Issue During Preceding 12 Months	No. Copies of Single Issue Published Nearest to Filing Date
a. Total Number of Copies *(Net press run)*	883	576
b. Paid and/or Requested Circulation (1) Paid/Requested Outside-County Mail Subscriptions Stated on Form 3541. *(Include advertiser's proof and exchange copies)*	547	415
(2) Paid In-County Subscriptions Stated on Form 3541 *(Include advertiser's proof and exchange copies)*	0	0
(3) Sales Through Dealers and Carriers, Street Vendors, Counter Sales, and Other Non-USPS Paid Distribution	48	50
(4) Other Classes Mailed Through the USPS	22	41
c. Total Paid and/or Requested Circulation *(Sum of 15b. (1), (2),(3),and (4))*	617	506
d. Free Distribution by Mail *(Samples, complimentary, and other free)* (1) Outside-County as Stated on Form 3541	17	16
(2) In-County as Stated on Form 3541	0	0
(3) Other Classes Mailed Through the USPS	0	0
e. Free Distribution Outside the Mail *(Carriers or other means)*	19	10
f. Total Free Distribution *(Sum of 15d. and 15e.)*	36	26
g. Total Distribution *(Sum of 15c. and 15f)*	653	532
h. Copies not Distributed	230	44
i. Total *(Sum of 15g. and h.)*	883	576
j. Percent Paid and/or Requested Circulation *(15c. divided by 15g. times 100)*	94%	95%

16. Publication of Statement of Ownership
☑ Publication required. Will be printed in the November 2013 issue of this publication. ☐ Publication not required.

17. Signature and Title of Editor, Publisher, Business Manager, or Owner — Date: 9/25/2013

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

Instructions to Publishers

1. Complete and file one copy of this form with your postmaster annually on or before October 1. Keep a copy of the completed form for your records.
2. In cases where the stockholder or security holder is a trustee, include in items 10 and 11 the name of the person or corporation for whom the trustee is acting. Also include the names and addresses of individuals who are stockholders who own or hold 1 percent or more of the total amount of bonds, mortgages, or other securities of the publishing corporation. In item 11, if none, check the box. Use blank sheets if more space is required.
3. Be sure to furnish all circulation information called for in item 15. Free circulation must be shown in items 15d, e, and f.
4. Item 15h., Copies not Distributed, must include (1) newsstand copies originally stated on Form 3541, and returned to the publisher, (2) estimated returns from news agents, and (3), copies for office use, leftovers, spoiled, and all other copies not distributed.
5. If the publication had Periodicals authorization as a general or requester publication, this Statement of Ownership, Management, and Circulation must be published; it must be printed in any issue in October or, if the publication is not published during October, the first issue printed after October.
6. In item 16, indicate the date of the issue in which this Statement of Ownership will be published.
7. Item 17 must be signed.

Failure to file or publish a statement of ownership may lead to suspension of Periodicals authorization.

PS Form **3526,** October 1999 *(Reverse)*

CNE QUESTIONS

1. **According to the proponents of mandatory alcohol and drug testing after adverse events, which of the following is true?**
   A. Research has shown a clear connection between impairment and adverse events.
   B. Research has shown a small, limited connection between impairment and adverse events.
   C. Research has shown a significant but not conclusive connection between impairment and adverse events.
   D. Research has not shown a connection between impairment and adverse events.

2. **According to Kathryn R. Coburn, JD, an attorney with the law firm of Kobrick and Wu in Los Angeles, when does the Americans with Disabilities Act apply to employees using drugs or alcohol?**
   A. It never applies.
   B. It does not apply those who "currently" abuse alcohol or drugs.
   C. It applies to all employees with drug or alcohol addiction.
   D. It applies only if the employee is actively in treatment for the addiction.

3. **In the updated Provider Self-Disclosure Protocol, what does the Office of Inspector General (OIG) state that self-reporting will presumptively indicate?**
   A. There is an effective compliance program, and no corporate integrity agreement (CIA) is needed.
   B. The violation occurred because there was no compliance program and a CIA is necessary.
   C. The disclosing party should be audited for further violations.
   D. The disclosing party has repaid the funds in question.

4. **In which of the following ways does Paul Hildebrand, MD, associate director of the patient safety organization TeamHealth in Knoxville, TN, suggest telemedicine might help reduce liability risks?**
   A. Providers can deliver care to patients in remote areas that those patients otherwise might not receive.
   B. Diagnoses by telemedicine are known to be more accurate.
   C. Patients are less likely to sue for errors that are associated with telemedicine.
   D. State laws provide strong defense for malpractice in telemedicine.

Legal Review & Commentary

A Monthly Supplement to HEALTHCARE RISK MANAGEMENT

$9 million awarded to patient after missed diagnosis of broken neck

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

Jamie Terrence, RN
Director of Risk Management Services
California Hospital Medical Center
Los Angeles

News: The patient presented to the hospital complaining of neck pain after being involved in an automobile accident. CT scan imaging was not performed on the neck/cervical spine. The patient was discharged home simply on the basis of a point tenderness examination in that area. Less than 48 hours later, while walking, he suddenly felt a shock of pain in his neck, and his left arm went numb. He was taken to the hospital, where a fracture in the cervical spine was revealed by X-rays. The patient's left arm sustained severe nerve damage and is essentially paralyzed, and his neck and left shoulder are in constant pain. The patient sued for negligence, and his wife asserted a claim for loss of consortium. The hospital and the doctor denied that the care was negligent. The jury sided with the patient and awarded $7 million in damages and another $2 million to the wife for loss of consortium. Both defendants are jointly and severally liable for 100% of the verdict.

Background: The patient, a man in his early 50s, was involved in an automobile accident in which the vehicle rolled twice. He presented to the emergency department complaining of neck pain. The patient contended that even though hospital policy was to perform CT scan imaging and obtain three views of the cervical spine when the patient had been involved in a high-energy trauma such as a motor vehicle accident, and even though CT scan imaging was performed on the head and middle back (thoracic spine), no such imaging was ordered on the neck and cervical spine. According to the doctor, the doctor simply performed a point tenderness examination in that area and concluded that the patient could be discharged home. The patient contended that no such point tenderness examination even took place.

"All of these problems could have been avoided if the cervical spine had been imaged ... and the fracture diagnosed ..."

Just two days later, while recovering at a friend's house, after spending most of the preceding 48 hours in bed, the patient walked to the bathroom and immediately felt a searing pain "like a bolt of lightning went off in my head." His left arm went numb. He returned to the hospital, where X-rays taken of his cervical spine for the first time showed a fracture around the fourth and fifth vertebrae of his cervical spine. He immediately underwent emergency surgery for his left arm, formerly his dominant arm, and remains essentially paralyzed in that arm. It appears the condition may be permanent. The patient also lives in constant neck and left shoulder pain, and the patient and his wife testified that their marriage has been significantly strained as a result of the physical and emotional toll of the events.

The patient and his wife sued for

Financial Disclosure: Executive Editor **Joy Daughtery Dickinson** and Nurse Planner **Maureen Archambault** report no consultant, stockholder, speaker's bureau, research, or other financial relationships with companies having ties to this field of study. **Damian Capozzola** and **Jamie Terrence,** co-authors, have no relevant relationships to disclose.

negligence and loss of consortium, respectively. In particular the patient claimed that the defendants (the hospital and the doctor) failed to properly diagnose his broken neck in the first instance. The patient claimed that when he subsequently started moving around 48 hours later, the damaged vertebrae shifted and impinged on a nearby nerve root, which caused significant nerve damage. All of these problems could have been avoided if the cervical spine had been imaged, pursuant to hospital protocols, and the fracture diagnosed, the patient claimed.

Also noteworthy in this particular case is that when the patient initially presented to the hospital, the lead doctor was the only doctor on duty supervising what already had been a busy morning in the emergency department. The lead doctor already had driven more than three hours to work, worked a full eight-hour shift, and was roughly three hours into an immediately following second shift, which suggests that the doctor might have been fatigued.

The defendants contended that the care provided had been proper. The jury ultimately agreed with the patient and his wife, and the jury awarded the patient $7 million in damage. The wife received $2 million in damages.

What this means to you: In any high-impact motor vehicle accident, first responders place victims on back boards and in C-collars to prevent further injury to the head, cervical, thoracic, and lumbar vertebrae. On arrival to the nearest trauma center, these life-saving devices are not removed until there is confirmation via X-ray, CT, MRI, or other imaging study that there has been no injury to these delicate structures. Even if the receiving hospital is not a trauma center, it does not negate the responsibility of the emergency department staff to follow this standard protocol.

Make sure that your hospital emergency department has these policies and procedures in place and that they are followed. It is not uncommon for hospitals to create policies with the best of intentions, but then fall short by not ensuring that all individuals affected by them are not only aware of them, but also well-trained to implement them. In this case, there was evidence of improper or incomplete training as well as a lack of follow through in the implementation of the protocols. If there are written policies that are not followed, it makes it easy for plaintiffs to allege negligence.

Also, there was some evidence in this case of nurses being afraid to insist on CT scan imaging of the cervical spine when the patient initially presented. One unwritten rule of risk management states that no critical decision should ever be left up to a single individual. For this reason, surgeons are never solely responsible for a sponge count, for example. The airline industry is another example where this rule applies. In emergency departments, doctors and nurses must "have each other's back." Nurses need to feel confident to express concerns in real time when policies are not being followed. This situation can happen only when the physicians they work with not only allow this practice, but encourage it and praise their colleagues for their teamwork and cooperation. In a punitive culture of physician dominance and tolerance of bad behavior, a nurse will be less likely to challenge the decisions of doctors who might not be following protocols for fear of reprisal.

Nurses and physicians also have a responsibility to bring concerns about their team members' personal behaviors forward to hospital leadership. In a true culture of safety, recognizing limitations that stressors place on healthcare workers is critical. Fatigue, family, and social pressures can weigh heavily on the physician or nurse's ability to function. Allowing the caregiver time off for a "mental health day," an extended leave, or even providing counseling should be an important part of a program to prevent an over-worked or overstressed professional from making an avoidable error. In this case, the judge did not allow the patient to present evidence of ongoing significant personal issues in the lead doctor's life at the time of the incident. However, in pretrial discovery, it was learned that the doctor was going through divorce proceedings and was scheduled to be deposed in those proceedings the next day. The judge determined that such evidence would be overly prejudicial to the defendants and excluded it from evidence. However, from a risk management perspective, it is natural to wonder whether the doctor's personal distractions played a role in the events and, in particular, in the decision not to order any imaging of the cervical spine.

Finally, note that Wyoming is generally known as a conservative venue, thus generally a good venue for defendants on the theory that Wyoming juries are unlikely to award large verdicts. It is hard to imagine, for example, that any lawyer or plaintiff receiving a favorable verdict in a notorious jurisdiction such as West Virginia or California ever said afterward, "If only we'd been in Wyoming!" However, here a Wyoming jury obviously did award a very significant sum. This case suggests that it is unwise to put too much stock in the reputation of the jurors of the venue if the facts of the case otherwise suggest that a major adverse verdict might be warranted.

Reference

Wyoming District Court Case No. 1:10-CV-00202-ABJ; 10th Circuit Court of Appeals Case Nos. 11-8102 & 12-8027 ✦

Family awarded $10.8 million after woman dies from complications following cardiac catheterization

News: A woman underwent routine cardiac catheterization in a hospital. Complications arose, and the patient died. The patient's family sued and contended that the hospital and the doctor did not take sufficiently prompt or adequate actions to treat the complications. The defendants contended that all reasonable and proper steps had been taken to care for the patient, who had suffered from a rare complication that was difficult to deal with. The jury sided with the patient's family and awarded $10.8 million. Both defendants are jointly and severally liable for 100% of the verdict.

Background: Cardiac catheterization is usually a relatively routine medical procedure used to diagnose and treat certain heart conditions. A catheter is essentially a long, thin, and flexible tube that is inserted through a blood vessel in the arm, neck, or groin and pushed through to the heart, which allows providers to perform treatments and do diagnostic tests. Although usually performed in a hospital setting by cardiologists, the patient remains awake during the procedure. It causes minimal if any pain, and rarely results in serious complications.

In this case, the patient was a woman in her mid-30s who, according to the patient's family, had a very mild history of heart issues. The woman initially went to a doctor complaining of possible bronchitis, but tests showed possible signs of heart trouble. She underwent a cardiac catheterization procedure. The cardiac catheterization procedure initially was believed to be routine and showed her heart was healthy and clear. However, during the procedure, one of the coronary arteries (left main) was dissected. This dissection means that the inner lining of the artery was disrupted by the tip of the catheter, which resulted in the collapse of the inner lining and a significant supply of blood to the heart being cut off.

The patient's family contended that once the patient started showing signs of severe complications post-catheterization, more than 30 minutes passed before the patient was taken for surgery. The patient's family said the patient was near death when she arrived for surgery 20 minutes later and nearly 50 minutes after complications arose. Despite three hours of surgical efforts, the patient died. The hospital and the doctor, an interventional cardiologist who is board-certified in internal medicine/cardiovascular disease, testified that all proper and reasonable efforts had been made to care for the patient in light of what they argued was a rare complication that was difficult to deal with. On an 11-1 vote, the jury sided with the patient's family and awarded $10.8 million dollars.

What this means to you: The facts of the case and size of the jury's award suggest that the defense never offered a good explanation for why an interventional cardiologist waited for such a long time to identify the severity of the problem and take appropriate action (i.e., ordering immediate surgery) once the patient started showing signs of disruption to a significant blood vessel. Some evidence uncovered during the discovery phase of the case suggested that in the past, the doctor had experienced a similar but less serious situation. Thus, the doctor might erroneously have believed that the patient here had more time than she did to see whether the symptoms would subside and to bring in his partner to consult, instead of acting immediately and decisively on the theory that one could assume only the worst.

Rigorously requiring even the most prestigious doctors working at a hospital to attend conferences and participate in periodic refresher and continuing education courses might help avoid a circumstance in which a highly regarded specialist makes a fundamental error with disastrous consequences.

The case also illustrates the potential danger of subjecting patients to unnecessary medical tests and procedures. Here we have an apparently healthy woman in her mid-30s who went to the emergency department complaining primarily of symptoms of bronchitis. The doctor prescribed albuterol. The patient complained of chest pains, which is a known side effect of albuterol. Because the patient had in the past some very mild heart issues related to an irregular heartbeat, the hospital decided that a cardiac catheterization was required. During that procedure, the left main coronary artery was disrupted, and the problem was not identified and remedied quickly

enough. By the time the patient reached the surgery room, not even three hours' worth of surgical efforts could save her life. The simplistic story is that she went in with a cough, got caught in a cascading series of medical misjudgments, and died in the care of her hospital doctors. Had monitoring or less invasive measuring techniques instead of full-blown cardiac catheterization been employed, the patient very well might have survived without any further incident at all.

That said, it is also worth noting that even one of the family's attorneys was subsequently quoted in the press as agreeing that was an isolated situation. Isolated situation or not, the jury still found the hospital and the doctor at fault and returned a very large verdict for the patient's family.

Always expect the unexpected when performing delicate invasive procedures on critical organs. It is rare that during a routine catheterization the catheter can cause a dissection. If this happens the interventional cardiologist will try and "repair" this problem with an angioplasty or stent. How unstable the patient becomes depends on the vessel that is dissecting. The left main would have a very high mortality. While the cardiologist is working on a "bail-out" or rescue intervention and probably inserting an intra-aortic balloon pump (IABP), the on-call cardiac surgical team will be alerted and on the way in for the emergency surgery needed to repair the damage. In most hospitals, a cardiac surgical team is on-call in the event of an unexpected emergency. In cases where there is increased risk of an untoward event, such as with a patient who has left ventricular dysfunction and an ejection fraction less than 30%, the interventional cardiologist can request that the cardiac surgical team be on site.

Your hospital can prepare by taking the following steps:

- Make sure that back-up systems are in place to call in staff.
- Know how to reach people quickly. Have current phone or pager numbers easily available.
- Have emergency equipment such as your "crash cart" IABP, suction, and supplies checked daily, and have it all close by and ready for use. Make sure staff knows how to use it.
- Run drills periodically to test staff competency.
- Have policies in place that speak to expected responses in emergency situations.
- Finally, have your physicians always educate patients on what risks are involved in these types of procedures and ensure that they have documented this information in the informed consent process.

Medical staffs should also review their credentialing processes to ensure that physicians who perform high-risk procedures are credentialed carefully, maintain their board certifications, and are consistently monitored for performance issues. A tight peer review process is critical if the hospital wants to safely offer advanced medical and surgical services to the community.

As in the first case discussed above, there is also a responsibility for the cardiac catheterization team to intervene on behalf of the patient if they think there is a delay to provide emergent care. Was the catheterization lab staff aware of the surgeon's delay? Did they "speak up"? All hospitals have a hierarchy or chain of command available to staff to use to bypass a provider who is not following a procedure or standard of care. In this case, there also was a responsibility for other team members to advocate for their patient.

The key legal question in any case like this one is whether the hospital, doctor, and staff behaved reasonably under the circumstances given the facts that were known to them at the time in light of their training, education, and institutional policies and expectations. Failing to speak up when a patient's life hangs in the balance will rarely look reasonable, and neither will the failure to have a process to allow people a safe outlet for raising legitimate concerns. It is important for risk managers at hospitals and medical clinics to work with their in-house legal counsel and develop constructive policies along these lines. If there are no in-house legal counsel or if the in-house legal counsel for whatever reason lack the expertise to advise authoritatively on these issues, strongly consider investing in the expertise of outside counsel experienced in these areas, where an ounce of prevention can be worth well more than a pound of cure.

Finally, the facts underlying this case raise many questions. Was the procedure even necessary? Why was there a rush to perform a cardiac catheterization after a complaint of chest pain without other findings? Did she have a questionable EKG? Was a stress test done that showed ischemic changes? Certainly the stress test could have been offered first. Perhaps her chest pain came from nothing more than her active cough. Bronchitis, before treatment, can be very painful in and of itself. Another rule of risk management is to start with and rule out the simplest explanation first before exploring the more complex. It often works. Disciplined implementation of such an active risk management approach also can be beneficial in any subsequent litigation, but it is critically important to document steps taken, results obtained, and the reasoning behind decisions as the treatment process moves forward.

Reference:

11SL-CC03684, Division 5, Circuit Court of St. Louis County, MO, 21st Judicial Circuit. ✦

HIPAA Regulatory Alert

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

Compliance accountability chains put you at risk and can complicate contract negotiations

Risk managers are doing the right thing when they try to include Health Insurance Portability and Accountability Act (HIPAA) compliance in vendor contracts, but they might meet resistance if the requirements are too onerous. The key will be finding the sweet spot where you have protected your interests as much as possible without making the contract untenable to business associates, experts say.

Resistance most likely will come from smaller companies, says **C. Jason Wang**, MD, PhD, associate professor of pediatrics at Stanford University in California. Wang recently wrote in the Journal of the American Medical Association (JAMA) that the 2013 HIPAA omnibus final rule creates an "unfunded mandate" on startup companies that might not have the wherewithal to negotiate business associate agreements.[1]

In the *JAMA* paper, Wang and his co-author call for additional guidance from the Department of Health and Human Services (HHS) on how contracts between healthcare entities their business associates should be construed. The final rule creates an accountability chain that includes business associates and their downstream subcontractors, Wang writes, but it does not account for what he says could be strong resistance from business associates.

Wang tells HIPAA Regulatory Alert that providers' worries about accountability could have the unintended consequence of limiting innovation and narrowing the field of companies with which a hospital is willing to work. If the hospital insists on strict compliance with HIPAA, evidence that the requirements have been passed down the line to subcontractors, and indemnity for violations, inevitably some companies will balk and say they cannot take on that responsibility, he explains. *(See the story on p. 3 for suggested contract clauses.)*

"I really worry that if this HIPAA regulation is interpreted too far, it's going to impede innovation and get in the way of providers working with outside companies," Wang says. "That will be terrible for healthcare."

Conflicts might be inevitable, but the provider still must follow the law and include contract clauses to protect itself from liability, explains **Stephen Wu**, JD, a partner with the law firm of Cooke Kobrick & Wu in Los Altos, CA. The HIPAA rule explains most of what should be required of business associates, but Wu advises risk managers to take a stricter approach in some areas. The rule requires that business associates notify the provider of a breach within 60 days, for example, but he advices hospitals to require must quicker notification. He has worked with one hospital that successfully negotiated a two-day notification from a data management company.

"You're probably going to get something more than two days, but it should be way south of 60," Wu says.

The flow-down requirement for subcontractors can be the stickiest negotiating point, Wu says. Flow-down means that once you contract with a business associate, your requirements for HIPAA compliance must be included in the contracts with any subcontractors and their subcontractors

Including flow-down is not optional, Wu says, but you have some discretion in what you flow down. You must consider your contract requirements not only in terms of whether the business associate is able to comply but also whether its

EXECUTIVE SUMMARY

Providers are accountable for the compliance of all downstream contractors with the Health Insurance Portability and Accountability Act (HIPAA). Vendors might balk at some efforts to ensure compliance.

- Covered entities can be responsible for the violations of business associates.
- The risk of liability is higher if the associate acts as an agent for the hospital.
- Some flexibility is necessary when negotiating HIPAA compliance clauses.

subcontractors can. "There are provisions that, in theory, should be flowed down to the business associates but which really aren't necessary when you consider the nature of the work. If the associate is handling patient data in a way that never involves them getting direct queries from patients, you could skip the provision about the associate being required to respond to requests by a certain time," he says. "You could take that off the table so they don't resist having to promise compliance on something they never do. But you could replace it with a clause saying they will cooperate fully if the patient makes a request to you and you need that information from them."

Money is always a sensitive topic, so indemnification and who pays for the breach of the protected health information can be difficult during negotiation, Wu says

In Wu's experience, the biggest controversy in these contract negotiations is the vendors claiming that they are not business associates at all. Contractors will argue that, for example, they merely maintain access to digital information for the provider but never open the files or have any knowledge of their contents. They will say that for that reason, they should not be considered business associates.

"You have to push back and tell them that because they are maintaining protected health information over time," Wu says. "That is the HHS decision, and they can't argue that point."

Wu advises risk managers to include a clause in the contract in which the vendor acknowledges being a business associate, along with a separate agreement to follow the compliance guidelines provided by the hospital.

One attorney urges risk managers not to go overboard with HIPAA compliance in contract negotiations. The legal risk to hospitals from missteps by business associates often is overstated, says **Brad Rostolsky**, JD, an associate with the law firm of Reed Smith in Philadelphia who has worked with healthcare providers to ensure data security. There is a risk of flow-down exposure, but that risk is significant only when the contractor is acting as an agent of the hospital, Rostolsky says.

"It is not true that contractors are generally on the hook for the actions of their business associates," he says. "We don't always have to negotiate as if something terrible is going to happen somewhere down the line and we're going to be liable to a great extent if we don't have a clause saying otherwise."

If a business associate is an agent under the federal common law of agency, then the covered entity is on the hook for the missteps of the business associate with regard to actions performed as an agent, Rostolsky says.

"When people try to implement more onerous language regarding indemnification and liability with business associates, I'd say that concern is valid up to a point, but may be a little misplaced," he says. "Don't be surprised when some of your associates come back to you and say that because of the cost of compliance they're going to have to raise their prices, or they're not going to be able to give you the indemnification you prefer."

Rostolsky advises structuring the contract up front so that, to the extent possible, the business associate is not an agent. To do so, the business associate must not be subject to direction by the covered entity on an ongoing basis. He cautions, however, that a single-minded focus on obtaining indemnification or other HIPAA concessions can backfire. "I've told people on both sides of this issue that if you push too hard, you can negotiate yourself out of business," he says. "Both parties in this negotiation have valid concerns and parameters for what makes good business sense, and you have to find somewhere to meet in the middle."

Covered entities also should be comforted by the fact that the government is going after business associates directly for HIPAA violations, Rostolsky says. That action doesn't mean they can't drag the covered entity into the fray as well, but Rostolsky says that will not be automatic if regulators can see that the associate was the responsible party and the covered entity acted properly in trying to ensure that the associate was in compliance.

As the Office of Civil Rights (OCR) continues enforcement activities against business associates, Rostolsky expects that "it will become implicitly clear that when a business does something improper, OCR will not hammer the covered entity for that unless there is an agent relationship."

REFERENCE

1. Wang CJ, Huang D. The HIPAA conundrum in the era of mobile health and communications. *JAMA* 2013; online Aug. 26. Accessed at http://jama.jamanetwork.com/article.aspx?articleid=1732507.

SOURCES

• **Brad Rostolsky**, JD, Associate, Reed Smith, Philadelphia. Telephone: (215) 851-8195. Email: brostolsky@reedsmith.com.
• **C. Jason Wang**, MD, PhD, Associate Professor, Stanford University, Stanford, CA. Telephone: (650) 736-0403. Email: cjwang1@stanford.edu.
• **Stephen Wu**, JD, Partner, Cooke Kobrick & Wu, Los Altos, CA. Telephone: (650) 618-1454. Email: swu@ckwlaw. ■

Contract clause samples for HIPAA chain

These sample contract clauses for ensuring business associates comply with the Health Insurance Portability and Accountability Act (HIPAA) are provided by **Stephen Wu**, JD, a partner with the law firm of Cooke Kobrick & Wu in Los Altos, CA:

• Acknowledgement of Business Associate Status.

Business Associate Status. The parties acknowledge that in connection with Services provided to Customer, Vendor is a "business associate" within the meaning of HIPAA. Vendor will comply with all requirements of HIPAA applicable to business associates in connection with the provision of its Services."

• Security obligation tied to HIPAA Security Rule.

Sample 1:

Business Associate agrees to: . . .

(b) Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement;…

Sample 2:

In delivering Services to Customer, Vendor will maintain reasonable and appropriate administrative, technical, and physical safeguards to comply with the HIPAA Security Rule, 45 C.F.R. §§ 164.302-164.318, including by the officers, members, employees, contractors, and subcontractors of Vendor.

• Security obligation untethered from a specific reference to the HIPAA Security Rule.

Vendor will maintain administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Services provided to Customer and the Customer Information stored on Vendor's systems; … ■

Prepare now for coming HIPAA security audits

It won't be long before someone knocks on your door and says it is time for a Health Insurance Portability and Accountability Act (HIPAA) security rule audit. What you do between now and then can determine how well that visit turns out for you.

The government is refining its audit protocol after testing it at 115 facilities, notes **Bruce D. Lamb**, JD, a shareholder with the Gunster law firm in Tampa Bay, FL. The Office of Civil Rights (OCR) at the Department of Health and Human Services (HHS) has stated that a permanent security audit program will begin Oct. 1, 2014. Some audits will be performed earlier than that as the OCR fine tunes its procedures.

"I expect some audits will be performed this year, with probably a pretty aggressive approach," he says.

The entities that are currently subject to audits are those that have certified compliance with the meaningful use criteria for electronic health records and received government funds for meeting that benchmark. During the testing, the procedure involved notifying the covered entity of an audit date, followed by an on-site inspection. There is no set time period for the length of the audit, but in the test audits so far, auditors were on-site for as long as five days.

The audit will begin with an interview of the privacy officer, and then the auditors will want to look at sample documentation. "They're not going to look just at rules and policies. They may ask for instances in which you released records to someone other than a patient," Lamb says. "Then they will check the adequacy of the documentation, whether you followed all the requirements to the letter."

Risk managers can use that same process in a mock audit to check their HIPAA compliance, Lamb suggests. A mock audit should include questioning hospital employees about policies and procedures for HIPAA compliance, because the real auditors certainly will. "They're not going to just look at your paperwork and talk to the compliance officer, the most knowledgeable person in the place about HIPAA," Lamb says. "They're going to walk up to medical records clerk and ask about certain tasks should be handled, and that person needs to be comfortable answering correctly. Most people need to be trained for that, or they'll trip up."

Lamb expects the HIPAA auditors to begin with

EXECUTIVE SUMMARY

Providers should plan now for the Health Insurance Portability and Accountability Act (HIPAA) audits that begin on a permanent basis Oct. 1, 2014. Different strategies are possible for having your organization ready when it is time for an audit.

- Some audits will happen much earlier as regulators refine the process.
- Large providers likely will be the first targets.
- Auditors might be on site as long as five days.

the largest covered entities, hospitals, rather than smaller providers such as physician groups. To prepare for audits, the first obvious concern is having your organization in compliance with HIPAA. That compliance includes having a HIPAA privacy officer.

Covered entities should review each of the obligations in the test auditing process, Lam advises. The protocol is available online at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html. Conduct a self-assessment for compliance and correct any deficiencies, and create a specific plan of correction for anything that cannot be resolved immediately.

"Business associate agreements will be a target in these audits. You're going to need to provide them a list of your agreements, and I think some hospitals are going to be lagging in this area and not able to hand those over in the correct form," Lamb says. "HITECH [Health Information Technology for Economic and Clinical Health rule] required a lot of changes in your business associate agreements, and I'm not sure everyone went back and revised those. There will be a focus on anything that has changed recently, and the biggest thing there is HITECH."

SOURCE

• **Bruce D. Lamb**, JD, Shareholder, Gunster, Tampa Bay, FL. Telephone: (813)222-6605. Email: blamb@gunster.com. ■

Advocate sued over large data breach

Advocate Health Care in Downers Grove, IL, and a subsidiary, Advocate Medical Group, are facing a state class-action lawsuit filed on behalf of two named plaintiffs and four million people whose protected health information (PHI) was taken along with four desktop computers in a burglary in July.

Advocate reports that the computers were password-protected but not encrypted. In a statement released after the breach was made public, an Advocate spokeswoman said Advocate had been working to encrypt its PHI since 2009.

A 12-page complaint in Cook County Circuit Court in Chicago alleges negligence, deceptive business practices, invasion of privacy, intentional infliction of emotional distress, and consumer fraud, all violations of Illinois law. Advocate's errors included "its use of nonsecure, unencrypted computers and software to maintain the private and confidential patient data," the complaint alleges.

The lawsuit requests a jury trial and judgment of an unspecified dollar amount for actual damages, costs, and other relief the court deems appropriate. According to the complaint, the plaintiffs' records were part of the July 15, 2013, data breach at an administrative office of the 1,100-plus physician Advocate Medical Group in Park Ridge, IL.

Advocate reports that the breach included more than four million records, making it one of the largest breaches by a healthcare provider since the federal government began requiring public reporting of larger healthcare records breaches in 2009. The breach is being investigated by the Office of Civil Rights of the Illinois Attorney General's office. ■

Agencies release model notices of privacy practices

Covered entities can now choose from three new models of Notice of Privacy Practices documents to maintain Health Insurance Portability and Accountability Act compliance (HIPAA).

The Department of Health and Human Services Office for Civil Rights (HHS OCR) and the National Coordinator for Health Information Technology released the model notices recently. Those agencies noted that they were created based on input from consumers and key stakeholders, and they reflect recent regulatory changes in the HIPAA Omnibus Rule. The notices come in three styles and are customizable, allowing providers to enter their own information prior to distributing and posting to the web.

The agencies said many entities have asked for additional guidance on how to create a clear, accessible notice that their patients or plan members can understand. In response, the agencies have provided separate models for health plans and healthcare providers. The three options are:

• Notice in the form of a booklet, or a notice with the design elements found in the booklet, but formatted for full-page presentation.

• A layered notice that presents a summary of the information on the first page, followed by the full content on the following pages;

• A text-only version of the notice.

The models reflect the regulatory changes of the Omnibus Rule and can serve as the baseline for covered entities working to come into compliance with the new requirements. In particular, the models highlight the new patient right to access their electronic information held in an electronic health record (EHR), if the provider has an EHR in their practice. Covered entities may use these models by entering their specific information into the model and then printing for distribution and posting on their websites.

More information on the privacy notice models, including templates to use in creating your own, is available at http://www.hhs.gov/ocr/privacy/hipaa/modelnotices.html. ■