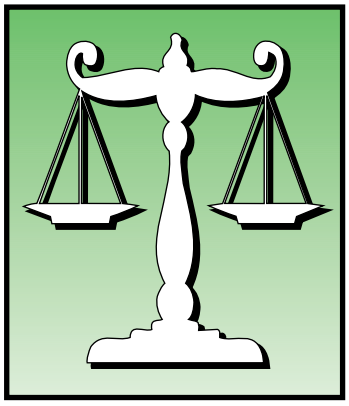
AMERICAN HEALTH CONSULTANTS®



Healthcare Risk Management™

INSIDE

DECEMBER 1998

VOL. 20, NO. 12 (pages 145-156)

American Health Consultants® is A Medical Economics Company

Sentinel event RCAs don't always lead to on-site review; reporting rules eased

Accreditation watch reserved only for uncooperative providers

Even though sentinel events and the resulting root cause analyses continue to strike fear in the hearts of risk managers, the good news from the Joint Commission on Accreditation of Healthcare Organizations is that most providers reporting their problems do not undergo an on-site review and only the uncooperative providers are likely to be put on accreditation watch.

There is still plenty of bite left in the sentinel event policy even as it evolves to accommodate some of the greatest fears of risk managers, but recent changes in the policy and declarations from Joint Commission officials may ease your mind a bit. Unlike when the policy was first put into effect, it now appears that you do not have to turn over a wealth of confidential information — a "malpractice kit for plaintiffs' attorneys," as some observers note. And you are not likely to suffer the grave indignity of accreditation watch status as long as you are making a good-faith effort to comply with the rules and help Joint Commission officials understand what happened.

> *"It's OK to show a root cause analysis for something like a near suicide or a medication error with no patient harm. That shows the Joint Commission your processes without exposing you to liability for disclosing that information."*

That was the message delivered to attendees of the recent meeting of the American Society for Healthcare Risk Management (ASHRM) in San Diego. At one of the most heavily attended meetings, risk managers listened closely, perhaps sometimes skeptically, to what the Joint Commission representative had to say about changes made to the policy only a few days before.

In the latest evolution of the policy, the Joint Commission provided one more option for how it might review a provider's root cause analysis — the report prepared by the provider after a sentinel event that is intended to ferret out the true, systematic cause of the event and highlight ways to

correct the problem. Risk managers have complained that the original policy required them to hand over, in the form of the root cause analysis, a great deal of information that would otherwise be confidential and unavailable to plaintiffs' attorneys. Previous changes to the policy were intended to address those concerns by providing options that did not involve handing over the root cause analysis.

Now the Joint Commission has added a fourth option with the same intent, says **Donna Nowakowski**, RN, director of government relations and external affairs for the Joint Commission.

She told ASHRM attendees that the fourth option was made official Oct. 1. A root cause analysis still is required after a sentinel event, but the new fourth option allows the provider to say that hospital officials will discuss policies and procedures and discuss their response to the sentinel event during an on-site visit by Joint Commission investigators but without seeing or even discussing the root cause analysis.

A previous modification allowed the option of discussing the root cause analysis on-site but without allowing it to leave the premises. Providers also can allow investigators to review the root cause analysis on-site, or they can just send it to the Joint Commission. **(For the exact wording of the options provided by the Joint Commission, see story, p. 147.)**

Accreditation watch not likely

Clearly trying to assuage the fears of risk managers, Nowakowski went on to say that the information in most root cause analyses does not lead the Joint Commission to pursue further on-site evaluation. Many analyses show that the incident in question does not even meet the criteria for a sentinel event, so the Joint Commission just informs the organization of that finding and drops the matter, she says.

She also explained that accreditation watch, the feared end result of a sentinel event investigation, is not likely even when the sentinel event is outrageously bad.

"Accreditation watch is limited to those organizations that don't share information with the Joint Commission," she says. "It's possible to put an organization on accreditation watch after giving it a chance to revise an unsatisfactory root cause analysis and still not getting an acceptable result, but in reality, it's for organizations that just don't share information."

The statistics provided by Nowakowski support that contention. Between March 1996 and March 1998, 139 providers survived the sentinel event investigation process without being put on accreditation watch. Another 37 organizations were placed on accreditation, and two were put on preliminary nonaccreditation. The numbers since March 1998 are a little different, and Nowakowski suggests that they more accurately reflect the current Joint Commission approach to sentinel events. Since March 1998, 63 organizations were investigated for sentinel events, and only one was placed on accreditation watch.

New option: Don't reveal root cause analysis

Nowakowski also assured risk managers that a root cause analysis will not have to be divulged during a routine triennial survey by the Joint Commission. Some risk managers have expressed concern that even if the root cause analysis of a sentinel event is not made available during the sentinel event investigation, a Joint Commission surveyor could demand to see all your root cause analyses as part of a routine survey to determine whether you are in compliance. But Nowakowski says the official Joint Commission position is that you do not have to hand over any particular analysis in that circumstance either.

Nowakowski emphasized that the surveyor may ask for all of your root cause analyses, but she says the provider has the right to deny the request and instead provide a sample root cause

analysis. The provider is free to choose a root cause analysis that is representative of the way it responds to sentinel events without including sensitive information.

"It's OK to show a root cause analysis for something like a near suicide or a medication error with no patient harm," she explained. "That shows the Joint Commission your processes without exposing you to liability for disclosing that information."

Differing legal risks from sentinel events

The Joint Commission's own investigation of how state laws affect the confidentiality of information in a root cause analysis suggests that there is, indeed, a myriad of laws and no easy answer. Legal officials in 44 states replied to the Joint Commission's survey, with seven indicating that sending a root cause analysis to the Joint Commission surveyors will not jeopardize confidentiality and another seven indicating that surveyor review of the root cause analysis on site, with the surveyor retaining a copy of the analysis, will not jeopardize confidentiality.

Twenty-four of the respondents (55%) said that confidentiality would not be jeopardized if the surveyor reviewed the root cause analysis on site without retaining a copy.

While much of Nowakowski's comments were greeted with relief from risk managers, a good deal of skepticism remained. Some of that skepticism was expressed by **Fay Rozovsky**, JD, MPH, DFASHRM, a risk management consultant in Richmond, VA. She also is chair of the ASHRM Sentinel Event Task Force and the ASHRM representative on the Joint Commission-American Hospital Association National Legal Task Force

Numbers show most reports from media

Inpatient suicides lead the statistics

At the recent meeting of the American Society for Healthcare Risk Management in San Diego, a representative presented some of the latest statistics from the Joint Commission on the Accreditation of Healthcare Organizations' sentinel events program. These are highlights presented by **Donna Nowakowski**, RN, director of government relations and external affairs for the Joint Commission:

There have been 332 sentinel events investigated by the Joint Commission to date, and of that number, Nowakowski had statistics for 287. The largest number of incidents, 57, were inpatient suicides, followed by 49 medication errors, 23 deaths related to a delay in treatment, 21 operative or postoperative complications, 20 deaths of patients in restraints, 17 events of surgery at the wrong site, 12 incidents of physical assault (including rape) or homicide, 11 transfusion-related deaths, 10 infant abductions or wrong discharges, six multistory patient falls, and five events involving medical gas systems.

The Joint Commission became aware of 41% of the incidents through the media, the most common way events were discovered, confirming the view of some skeptics that the sentinel event policy just plays on the sensational accidents reported by the news media. Another 29% were self-reported, but Nowakowski says the next update of the statistics probably will show that media reports and self-reports now account for close to equal portions of sentinel events because providers are more proactive in reporting their own events.

Twenty-one percent were discovered during a Joint Commission survey, 2% were reported by the patient or a family member, and 1% by an employee of the provider. Five percent were reported by some other method, such as a government agency or an anonymous report.

As some would expect, about 60% of the events occurred in a general hospital setting, followed by 22% in a psychiatric hospital, 8% in a psychiatric unit, 4% in an emergency department, 2% in an outpatient behavioral health center, 2% in a home care service, 1% in a long-term care facility, 1% in an ambulatory care setting, and 0.3% (one incident) in a clinical laboratory.

In the 287 incidents, a total of 334 patients were affected and there were 269 deaths. There was major loss of function in 14 incidents. Orientation and training deficiencies were identified as the root cause in most analyses, followed by communication and the patient assessment process. ■

that has been addressing risk managers' concerns about the sentinel event policy.

Rozovsky says there may be an unofficial fifth option when responding to a sentinel event, beyond the four options involving the root cause analysis.

"The fifth option would be the hospital board respectfully saying, 'we will not participate because we see no basis for the sentinel event allegation,'" she said. "That probably would lead to accreditation watch and possibly non-accreditation, but I think it has to be considered another option when responding."

Rozovsky also says the new fourth option — discussing policies and procedures with the Joint Commission surveyor without discussing or sharing the root cause analysis — may not work for some providers.

"If the Joint Commission decides what you've done is not enough, they can demand a focused review with more documents," she says. "If those documents are the ones you were trying to protect in the first place, you haven't accomplished anything and you're paying for the visits."

Concerns remain with sentinel event policy

Though she praised the way the Joint Commission had worked to accommodate the concerns of risk managers, Rozovsky said many problems remained. For instance, she said the 45-day rule for responding with a root cause

Legal reasons to offer options for reviewing sentinel events

The following are the newly revised options for how the Joint Commission on the Accreditation of Healthcare Organizations may review a provider's documentation concerning a sentinel event:

Alternatively, if the organization has concerns about increased risk of legal exposure as a result of sending the root cause analysis documents to the Joint Commission, the following procedures for review of the organization's response to the sentinel event are available:

1. Review of root cause analysis documents brought to Joint Commission headquarters by organization staff, then taken back to the organization on the same day.

2. An on-site visit by a specially trained surveyor to review the root cause analysis and action plan. The organization will be assessed a charge sufficient to cover the average direct costs of the visit.

3. An on-site visit by a specially trained surveyor to review the root cause analysis process and findings, without directly viewing the root cause analysis documents, through a series of interviews and review of relevant documentation. For purposes of this review activity, relevant documentation includes, at a minimum, any documentation relevant to the organization's process for responding to sentinel events, and the action plan resulting from the analysis of the subject sentinel event (to serve as the basis for appropriate follow-up activity). The organization will be assessed a charge sufficient to cover the average direct costs of the visit.

4. Where the organization affirms that it meets specified criteria respecting the risk of waiving legal protection for root cause analysis information shared with the Joint Commission, an on-site visit by a specially trained surveyor to conduct interviews and review relevant documentation to obtain information about:

- the process the organization uses in responding to sentinel events;
- the relevant policies and procedures preceding and following the organization's review of the specific event, and the implementation thereof, sufficient to permit inferences about the adequacy of the organization's response to the sentinel event. The organization will be assessed a charge sufficient to cover the average direct costs of the visit.

A request for review of an organization's response to a sentinel event using any of these alternative approaches must be received by the Joint Commission at least 15 days prior to the due date for the root cause analysis and action plan. ■

analysis is too short a time frame if any sort of criminal investigation also is involved.

"You can't get in the way of forensic evidence, and believe me, if it comes to disappointing the Joint Commission or having the local police charge me with obstructing their investigation, I know what choice I'm making," she says. "In some cases, the constraints of a criminal investigation can even prevent you from getting enough information to make the five-day reporting rule."

Rozovsky also points out that the process of conducting a root cause analysis could result in an emotional distress claim being filed against the provider by an employee. The analysis often requires those involved in the incident to relive it again and again by explaining it and dissecting each little portion. For an especially tragic or scary event, that could traumatize the patient so much that he or she would end up filing an emotional distress claim.

Rozovsky also points out that some medical staff will refuse to participate in the extensive research required for the root cause analysis if your medical staff bylaws do not require them to participate.

She suggests checking your bylaws to see if medical staff would be obligated to participate, and if not, you should change the bylaws. Physicians and nurses usually will be advised to keep their mouths shut about any incident likely to involve a lawsuit, so don't be surprised if they say the root cause analysis is beyond the clinical investigation to which they feel obligated.

Also, Rozovsky says she fears if an employee feels backed into a corner by the root cause analysis, he or she could respond by filing a qui tam lawsuit to expose some alleged misconduct at the hospital. That is most likely when the analysis seems to be heading in a direction that would single out an individual as the responsible party in the sentinel event, even if the failing ultimately is traced to a systemic shortcoming.

For More Information

- ❒ **Donna Nowakowski**, Joint Commission on Accreditation of Healthcare Organizations 1 Renaissance Blvd, Oakbrook Terrace, IL 60181. Telephone: (630) 792-5000.
- ❒ **Fay Rozovsky**, 12317 Pleasant Lake Terrace, Richmond, VA 23233. Telephone: (804) 364-2956.

For more information about the Joint Commission's Sentinel Event Policy and Procedures, visit the Joint Commission's Web site at jcaho.org or call the Sentinel Event Hot Line at (630) 792-3700. ■

Shady accounting common in health care

Latest allegations probably will lead to more

The latest federal charges against the Columbia/HCA Healthcare Corporation and the Quorum Health Group probably are only the first in a coming wave of allegations related to keeping double sets of books in an effort to fraudulently increase revenue, according to one insider. The practice has been widely accepted in health care accounting for years, he says, but now the government is catching on and planning a strong attack.

That prediction can leave risk managers in a difficult position because the creative accounting practices usually are well out of your control, yet they represent a clear risk to the institution. In some cases, you may find yourself obligated to march into the CEO's office and recommend that the hospital give up millions of dollars in revenue it earned just by changing a few numbers on a few documents.

"There is a lot of this going on out there," says **John Phillips**, JD, an attorney with the law firm of Phillips & Cohen in Washington, DC. Phillips & Cohen specializes in representing whistleblowers in False Claims Act cases. Their cases are responsible for about two-thirds of the $1.3 billion the government has collected through whistle-blower lawsuits in the last five years. "The government is now attuned to this issue and investigating it quite vigorously. We'll be seeing more examples of this soon."

Phillips & Cohen represents the whistle-blower who brought the charges against Quorum. It also turns out that the whistle-blower responsible for these allegations prompted most of the federal government's investigations of Columbia/HCA over the past few years. **(For more information on the whistle-blower, see story, p. 150.)**

In October, the federal government announced it was suing Columbia/HCA and Quorum for purposely defrauding the government with a

Whistle-blower filed qui tam in Columbia/HCA suit

Perhaps the most important lesson from the recent allegations against Columbia / HCA and Quorum is the power of the little guy: Everywhere throughout your institution are hundreds or thousands of people who each have the power to bring the full force of a federal investigation against you.

Remember that when you ask them to do things that might not be quite proper.

The allegations of keeping a double set of accounting books — one showing the true costs of care and one showing the inflated costs reported for reimbursement — all flowed from the qui tam lawsuit filed by James Alderson, a hospital accountant once employed at North Valley Hospital in Butte, MT.

Alderson claims that after the hospital was acquired by Quorum (a spinoff of Columbia / HCA) in 1990, he was instructed to create two sets of books. He refused, saying that two cost reports would be fraudulent and violate his code of ethics as an accountant.

Soon after, Alderson was fired. He filed a wrongful termination suit, and in the process, obtained copies of cost reports and reserve reports from Quorum. Alderson contacted the Justice Department in 1992 to advise that he was going to file a whistle-blower lawsuit alleging fraud and then filed suit in January 1993. The government immediately began demanding documents from the companies.

Identity just revealed

Alderson's complaint and the documents obtained in the subsequent investigation played a major role in the feds' much ballyhooed investigation of Columbia / HCA over the past couple of years, and it was a major impetus for the July 16, 1997, raid on Columbia / HCA facilities.

Alderson's identity and motivation were not known until the government unsealed his complaint on Oct. 5, 1998, and announced the lawsuit against the companies. ■

scheme that involved routinely overstating expenses to increase compensation from Medicare and other government programs. In addition to the corporate parents, more than 200 hospitals in 37 states are defendants. The lawsuits allege that the providers kept a secret second set of cost reports and work sheets that showed significantly lower expenses — the true expenses, according to the government — than the expenses submitted for reimbursement. Columbia / HCA and Quorum both responded to the charges with statements denying any intentional deception.

The use of reserve reports, the term accountants use for such second sets, is a tricky issue, Phillips says. Reputable accountants commonly use techniques that the average person would find confusing at best, and many of them can at least have the appearance of deliberate misdirection. The important point can be just how aggressive the company is with the reserve reports, Phillips says. With Columbia / HCA and Quorum, he says upper management stepped way over the line into fraud.

Cost reporting has always been the "obscure, backwaters of the accounting process," Phillips says. There had not been any fraud allegations regarding cost reporting in health care for years, so many providers began to see overstating cost reports as an easy way to increase their reimbursement from Medicare. The only risk seemed to be that the provider may be caught during an audit, but only about 25% of providers ever had their cost reports audited. And even when they got caught, the providers just had to pay back the disputed amount from a few years back with no interest, he explains.

"Providers were lulled into using this as a new source of revenue with low risk," he says. "When you have that situation occur with high potential and low risk, people are going to take advantage of it, especially the for-profit hospitals. This was an easy place to look for more money."

Phillips contends that Columbia / HCA and Quorum became so complacent about the practice that they thoroughly documented their fraud. The companies needed to know, partly for projections about future earnings, what their true costs were vs. the costs they were reporting to the government. So they kept two sets of books that clearly outlined what they were doing, he says.

"It has turned out to be like the Rosetta stone," he says. "There's nothing inherently wrong with reserve cost reports, but what is unusual is the level of detail that clearly indicates a degree of

knowledge that they knew these items were not proper for including in the cost report.

"They were even stamped on the front, 'Do not show to Medicare auditors,'" Phillips says.

Other providers may be doing the same thing

The same accounting practices probably can be found in many hospitals and systems across the country, Phillips says. Columbia/HCA and Quorum may be exceptional in the degree to which they supposedly documented the fraud, but he says "this is not an unusual example. The likelihood is that this is widespread."

That means risk managers should take a look at their institutions' accounting practices. These recent allegations are a major warning that similar charges are on the way, Phillips says. Risk managers would be well advised to find out what type of accounting practices are used in their facilities and try to head off any government charges, he advises.

"Voluntary disclosure is the way to go if you think you have exposure. The government will treat you much better," he says. "You can take the risk that nobody will ever know and you can keep the money, but your chances of getting away with that are much less than they might have been years ago."

If you investigate the paper trail and find something that makes your heart stop, you are obligated to act even if you think accounting practices are far beyond your sphere of influence, says **Grena Porto**, RN, ARM, DFASHRM, director of clinical risk management and loss prevention services at VHA Inc. in Berwyn, PA, and president of the American Society for Healthcare Risk Management (ASHRM). These tricky accounting practices usually are approved at the very highest levels of administration, and because they involve millions of dollars in essentially free money, it is reasonable for a risk manager to fear being laughed out of the CEO's office when you suggest stopping the practice.

"If you've got knowledge of something like this, you have to do something about it," Porto says. "Even if it were not a legal obligation, there is a moral and ethical obligation. And I can tell you that ASHRM would expect its members to do that."

Porto says she hopes there would be enough awareness about the risk of fraud these days that a risk manager would be received well when bringing such an issue to upper management. But she also acknowledges that the concerns may be dismissed when so much money is at stake. She suggests that the risk manager probably should take his or her concerns to the compliance officer, not necessarily the CEO, and report them as a compliance issue.

And conversely, she advises risk managers to take the issue seriously if anyone else brings the issue to them. "Sit up and listen when somebody comes in and reports this. If a person reports this and doesn't get a reasonable response, this is what makes them whistle-blowers," Porto says. "Honestly, I'm shocked to hear the allegations of what Columbia has done. Some of this stuff was so wrong that it makes us all look bad as health care professionals. I was professionally embarrassed by it." ■

For More Information

- **John Phillips**, Phillips & Cohen, 2000 Massachusetts Ave. NW, First Floor, Washington, DC 20036. Telephone: (202) 833-4567.
- **Grena Porto**, VHA Inc., 200 Berwyn Park, Suite 202, Berwyn, PA 19312. Telephone: (610) 296-2558.

Y2K should keep risk managers awake at night

If you have downplayed the potential effects of the year 2000 (Y2K) problem at your facility, you may be in for a nightmare — while everyone else is out celebrating the New Year — eighteen months from now. The Y2K problem is going to hit health care facilities hard, according to two experts who spoke at the recent meeting of the American Society for Healthcare Risk Management (ASHRM) in San Diego.

The problems are inevitable even if you are seriously addressing the problem right now, said **William McDonough**, MPAH, ARM, FASHRM, vice president and national health care risk management practice leader for Johnson & Higgins National Health Group in Boston. He speaks frequently on the Y2K problem in health care facilities, and the advice he had for risk managers was not at all comforting.

"My advice for what you can do? Buy a new filing cabinet for all those claims that are going to come in," he says. "You should count on lawsuits, business failures, board resignations, and shareholder loss of confidence."

Y2K computer glitches will lead to a rash of claims against the facility for failure to treat, failure to diagnose, and failure to monitor, he said. But on the other hand, McDonough said he does not expect a dramatic increase in medical malpractice claims from bodily injury. Those claims already are common, and the Y2K problem will happen essentially on just one day. Some computer repercussions, such as losing scheduling data, can have a ripple effect that will affect efforts to follow up on test results, for instance, so there will be an increase in that kind of lawsuit. Claims for actual injuries resulting from the Y2K glitch likely will not be all that numerous, he said.

"My advice for what you can do? Buy a new filing cabinet for all those claims that are going to come in. You should count on lawsuits, business failures, board resignations, and shareholder loss of confidence."

But that doesn't mean they won't happen. In fact, he predicts that there will be plenty of incidents in which ventilators will shut off or infusion pumps will work improperly, for example, and patients will be injured. The potential effect on an individual patient is enormous, he said.

"There will be deaths, no doubt about it," he predicted. "These are the things that should be keeping you awake at night."

The Y2K problem, also known as the millennium bug, results when a computer is programmed to assume that the first two digits in any date are 19. When the actual date rolls over to 2000, the computer may mistakenly think the year is 1900. Any dates programmed into the computer may be interpreted as 1901, for instance, instead of 2001. Or the computer could just become fatally confused and shut down.

McDonough said most health care facilities will encounter significant Y2K problems, but the difference will be the degree. If you are well on your way to addressing the problem by now, it is possible that you will be able to minimize the effect on your organization. If you haven't started, or if you're not making much progress by now — well, maybe you should buy several filing cabinets.

It's probably too late to hire a computer consultant to fix your facility's Y2K problems. There just aren't enough qualified consultants to go around. At this point, you're better off concentrating on your internal response to the problem, which could include hiring a full-time computer consultant.

In addition, McDonough made these recommendations:

❒ **Beware of exclusion language from medical malpractice carriers.**

Almost all states now allow language in medical malpractice policies that let the carriers off the hook for any computer-related medical injuries. Watch carefully for any changes in your policies, McDonough cautioned. Your insurer will want to slip this past you so that any liability rests entirely with your facility.

❒ **Realize that any alteration to your equipment absolves the manufacturer of liability — and most equipment has been altered.**

In most facilities, about 90% of your software has been "tweaked" to customize it to your needs, he noted. Contracts almost always state that the manufacturer has no responsibility for subsequent problems once you do that. "That means you cannot count at all on passing liabilities back to the vendor," he said.

❒ **Don't depend too much on compliance letters from vendors.**

You've probably already thought about getting compliance letters from vendors, attesting to their Y2K readiness. That's fine, but don't count on them too much. You also need to seek independent validity testing and third-party endorsement.

"That's so you can say to the plaintiff's attorney that you did not just rely on the vendor's letter," McDonough said.

Embedded chips mean problem's everywhere

Many of McDonough's words of caution were underscored by **Tony Montagnolo**, MS, vice president of technology planning for ECRI, the independent health care research institution in Plymouth Meeting, PA.

He confirmed that the number of potential Y2K problems in any one facility is almost impossible to calculate because there are so many devices that have embedded computer chips that could be affected. Even if the device appears to be not

For More Information

- **William McDonough**, Johnson & Higgins National Health Group, 200 Clarendon St., Boston, MA 02116. Telephone: (617) 421-0200.
- **Tony Montagnolo**, ECRI, 5200 Butler Pike, Plymouth Meeting, PA 19462. Telephone: (610) 825-6000.

much of a "computer," it may depend on an embedded chip that will be affected.

"Even if your ventilator has no place to punch in the date, embedded chips still can affect it," he said. "And you can't really test embedded chips. There are just too many of them."

ECRI's investigations have revealed that about 15% of all hospital equipment will be affected by the Y2K problem. Some of those problems will be minor, like an incorrect date printed on a form, and some will be major, like a defibrillator that will not activate because it thinks it was last tested in 1900. Montagnolo said this is ECRI's advice for risk managers:

- ❒ Take inventory, and prioritize your response.
- ❒ Perform a legal audit.
- ❒ Contact suppliers to see what they are doing.
- ❒ Test equipment.
- ❒ Repair or replace problem equipment.
- ❒ Hold your breath, and say your prayers.

Be careful with tests that could backfire

The inventory phase should include anything that has batteries or an electrical cord, he said. That is a huge number of items in your facility. Include all of those items, whether you own them or not.

"Watch out for the secret stash of devices, too," he said. "Everyone knows tales of restrooms that have been out of order for months and when you look inside, you find it's the secret stash of infusion pumps that the nurses squirreled away for when they really need them."

Your inventory should result in a high-, medium-, and low-risk assessment that you can use to prioritize testing and repairs. Montagnolo said high risks are "things that will kill you quickly," such as anesthesia machines and infusion pumps. Medium risks are "things that will kill you slowly," and low risks are "things that probably won't kill you even if they malfunction."

Once you get to the testing phase, be very careful. McDonough and Montagnolo both told stories of health care providers who were trying to check equipment for Y2K problems and found that their tests backfired on them. In one case, Montagnolo said a hospital was testing an MRI unit and rolled the date up to Jan. 1, 2000. Once staff saw how the machine responded, they tried to set it back to the correct date. It wouldn't go back.

In another case, McDonough said a hospital tried to test an entire operating room and ambulatory care center by shutting it down on a Friday night. The tests went fine over the weekend, and the OR opened for business on Monday morning. But then an infection control nurse did a routine check and found lots of bad bugs and mold. The problem? They had shut down the heating and air conditioning system during the test and the normally stable OR temperatures fluctuated.

"They had to close the OR and ambulatory care center for nine days, and their CEO was very upset," he says. "Always include the infection control nurse in plans like this. It's an example of how far-reaching the Y2K problem can be." ■

ASHRM responds to TV autopsy segment

A recent episode of *60 Minutes* on CBS has prompted the American Society for Healthcare Risk Management (ASHRM) to issue a public protest of comments that accused the risk management profession of widespread deception of patients and participation in a coverup of medical errors.

The segment aired Oct. 11 and focused on the nationwide decline in autopsies. Reporter Mike Wallace claimed that hospitals were intentionally discouraging autopsies due to fears of malpractice claims. **George Lundberg**, MD, the editor of the *Journal of the American Medical Association,* was interviewed and made comments critical of risk managers, including an anecdote about a risk manager masquerading as a grief counselor in order to deceptively urge a family against a "truth-finding" autopsy.

ASHRM president at the time the program aired, **Leilani Kicklighter**, RN, ARM, MBA, DFASHRM, responded with a letter to *60 Minutes*. In particular, she criticized the

allegation that risk managers suppress autopsies to avoid malpractice claims, and a statement from *JAMA's* Lundberg that, "Risk management, in many institutions in this country, is designed to suppress truth."

Both statements reflect a severe lack of knowledge about the risk management profession, Kicklighter wrote. Any effort to discourage autopsies would be unethical, and risk managers usually are not involved in that decision, she says.

"To blame health care risk managers for the declining autopsy rate, or worse yet, to accuse them of being part of a broad conspiracy to suppress information about causes of death, is inaccurate and irresponsible," she says.

The American Medical Association released a statement distancing itself from Lundberg's comments. In that statement, **Randolph Smoak Jr**, MD, chair of the AMA's board of trustees, says that Lundberg spoke as an individual and his comments do not represent the AMA's position. "It's irresponsible and unsupported to assert that malpractice is the reason the rate of autopsies is declining," Smoak says.

It should be noted, however, that Smoak's near-apology addressed only Lundberg's disparagement of physicians, not risk managers. The AMA did not respond to requests from *Healthcare Risk Management* for further comment concerning the allegations about risk managers. ■

Feds likely to pre-empt state confidentiality

Here's a heads-up for risk managers who have depended on their state confidentiality laws to determine some of their institution's policies on medical records. Everything you know may be about to change.

Federal efforts to enact confidentiality laws probably will come to a head in the next session of Congress, and you'll be better off if you know what's coming. Activists on both sides of the issue say it is likely that federal legislation soon will pre-empt state confidentiality laws, but opinions differ sharply on whether that is going to be a good thing or a bad thing.

Depending on who you listen to, the federal pre-emption could be either a big step forward from a mishmash of state laws that sometimes don't offer enough protection, or a concession to managed care plans that will rob patients of much of their privacy rights.

Efforts to enact federal legislation that would, in one way or another, pre-empt state confidentiality laws have been around for years, starting as early as the Carter administration. The federal government offered a model of uniform state legislation that could be enacted to eliminate the many discrepancies in the 1980s, but states did not adopt the model. The 105th Congress just toyed with the idea again by trying to pass several bills that would have involved creating federal laws that usurp state confidentiality laws, but the bills did not pass before the session ended.

Now it looks as if the next session of Congress will see some sort of action on the matter. Exactly what will happen is still to be seen, but most observers agree that state confidentiality laws will be addressed in some way. Either Congress will pass a law that pre-empts federal legislation, extend the deadline it is under for addressing confidentiality concerns, or just punt the matter on to the secretary of Health and Human Services (HHS).

The deadline imposed by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) will force some resolution of the issue, says **Kathleen Frawley**, JD, MS, RRA, vice president of legislative and public policy services with the American Health Information Management Association in Washington, DC. HIPAA requires Congress to pass legislation regarding uniform state confidentiality laws by August 1999.

"I've been involved in this issue for seven years, and I'm surprised that it is taking this long to get something done on a federal level," Frawley says. "We'll probably get something done in the next Congress because they have to. They could extend the deadline, but if they can't settle on legislation, I think they're more likely to let the Health and Human Services secretary do it."

Shalala could strike moderate position

If the Congress punts the issue to HHS Secretary Donna Shalala, the result may be a change that falls somewhere between the extremes of the debate. In her recommendation to Congress required by HIPAA, Shalala said on

Sep. 11, 1997, that the country does need a new national standard for protecting the privacy of health information.

She went on to say that, under her recommendation, "This new national standard would not limit or reduce other stronger legal protections for confidentiality of health information. Stronger state laws [such as those covering mental health and HIV infection and AIDS information] would continue to apply."

Federal law and state law would apply simultaneously so that if either forbade disclosure of the information, it could not be disclosed. The goal would be what Shalala calls "floor pre-emption" of state laws, so that everyone is ensured the protection afforded in the federal law. But in some cases, they would be afforded an extra measure of protection from their own state laws.

"Floor pre-emption" is a goal that seems acceptable to those on both sides of the debate, with some seeing it as the most they would accept and others seeing it as the least they would accept. On one side of the debate is **Donald Palmisano**, MD, JD, a member of the American Medical Association (AMA) Board of Trustees and a surgeon in New Orleans. Representing the official views of the AMA, Palmisano is a strong opponent of any measure that would threaten the privacy of medical records. He says floor pre-emption might be the way to settle the debate.

"We have seen bills so far that handled the issue in different ways, with some establishing a ceiling and some establishing a floor," he says. "We say it must be a floor. We support efforts that improve the protection of medical information, but some of the proposals have sacrificed some state confidentiality laws in favor of uniformity. Uniformity is not sufficient cause to weaken a state's laws."

The AMA could support federal legislation that would establish more privacy protection than is currently found in any state, but Palmisano says that is not likely.

Could this affect how patients talk to docs?

Much of Palmisano's concerns about federal pre-emption are related to the way patients must confide in their doctors regarding some delicate health matters. If federal laws take away some rights to the confidentiality of that information, patients may be reluctant to tell their doctors about mental health problems, drug and alcohol abuse, and similar issues that they may want to keep private. Some proposed legislation has included provisions that would allow managed care companies to collect such data on a routine basis without obtaining specific permission from the patient, sometimes for the purpose of accounting research, marketing, medical research, law enforcement, or other needs that do not directly benefit the patient.

"We recognize the importance of medical research and don't want to impede it. We also recognize the importance of technological efficiency, but those needs do not supersede the patient's right to confidentiality of health information," Palmisano says. "We're not Luddites. We're not anti-technology, but at the same time, we don't want to violate basic rights of our patients just because that makes it easier to use some types of technology."

In particular, Palmisano says that whatever law is passed should not put the burden on the patient to prevent the release of information. Patients will be harmed, he says, by catchall phrases that would allow the health care plan to use information about patients "to further the

Healthcare Risk Management (ISSN 0199-6312), including **HRM Legal Review & Commentary**, is published monthly by American Health Consultants®, 3525 Piedmont Road, Building Six, Suite 400, Atlanta, GA 30305. Telephone: (404) 262-7436. Periodical postage paid at Atlanta, GA 30304. POSTMASTER: Send address changes to **Healthcare Risk Management**, P.O. Box 740059, Atlanta, GA 30374.

Subscriber Information

Customer Service: (800) 688-2421 or fax (800) 284-3291, (custserv @ahcpub.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), $439. Outside U.S., add $30 per year, total prepaid in U.S. funds. One to nine additional copies, $220 per year; 10 or more additional copies, $132 per year. Missing issues will be fulfilled by customer service free of charge when contacted within 1 month of the missing issue date. **Back issues**, when available, are $38 each. (GST registration number R128870672.)

Editor: **Greg Freeman**, (404) 320-6361.
Publisher: **Brenda Mooney**, (404) 262-5403, (brenda.mooney@medec.com).
Executive Editor: **Susan Hasty**, (404) 262-5456, (susan.hasty@medec.com).
Production Editor: **Ann Duncan**.

Editorial Questions

For questions or comments, call **Greg Freeman** at (404) 320-6361.

For More Information

- ❒ **Kathleen Frawley**, American Health Information Management Association, 1225 I St. NW, Suite 500, Washington, DC 20005. E-mail: Kfrawley@ahima.org.
- ❑ **Donald Palmisano**, 4417 Lorino St., Suite 200, Metairie, LA 70006. Telephone: (312) 464-4016.

activities of the health plan," for instance. Patients also should not be asked to sign a blanket statement that allows the health plan to use information in that way, he says.

"We don't want any kind of default in favor of the insurance company so that the patient has to protest if he doesn't want information used in that way," Palmisano says. "Whatever the phrasing, it should put the burden on the health care plan to ask for that information if it wants to use it some way."

Frawley does not dispute much of what Palmisano says about the need to protect patient privacy, but she says you must remember that the nature of health care and management of medical records has changed dramatically in recent years. Information is flowing between states much more than it did previously because of the upsurge in managed care, so matters are complicated by conflicting state laws.

"Our recommendation would be to get the strongest federal regulation possible and you wouldn't need the state legislation," she says. "States are all over the place in terms of what they've done. If one rule applies in this state, what happens when that information goes to an insurer in another state? The notion of preserving existing state statutes and protections is probably comforting to individuals, but it doesn't give the patient better protection."

Interstate commerce often can leave insurers, providers, and patients wondering what restrictions apply to a particular situation, and Frawley points out that the individual patient rarely is present or capable of arguing about the fine points of one state law vs. another. A strong federal law would eliminate the ambiguity and protect the patient, she says.

"A lot of other issues have been worked out in the previous bills we've seen, but pre-emption is a very complex issue," she says. "States are responsible for the health of their citizens, so Congress is reluctant to intrude in an area that has long been reserved for state action." ■