Specialized Information Publishers Association Winner

Healthcare Risk Management™

AHC Media LLC

IN THIS ISSUE

Financial Disclosure: Author Greg Freeman, Editorial Group Head Russ Underwood, Managing Editor Karen Young, Nurse Planner Maureen Archambault, and *Legal Review & Commentary's* authors Blake Delaney and Jon T. Gatto report no consultant, stockholder, speaker's bureau, research, or other financial relationships with companies having ties to this field of study.

NOVEMBER 2008
VOL. 30, NO. 11 • (pages 121-132)

Hospital agrees to pay $89 million in False Claims Act settlement

Large payout holds lessons for risk managers

A False Claims Act (FCA) settlement totaling $89 million is ringing alarm bells in health care institutions across the country, reminding risk managers that improper billing and coding — or even carelessness that gives the impression of fraud — can result in a huge monetary loss when all is revealed to the feds. And the recent settlement highlights another reason to lay awake at night: Now the states have an incentive to dig deeper and get their own slice of the settlement pie.

In what the Justice Department says is one of the largest civil fraud recoveries ever against a single U.S. hospital, Staten Island University Hospital (SIUH) has agreed to pay the United States $74,032,565 to settle claims that the hospital defrauded Medicare, Medicaid, and the military's health insurance program, TRICARE. The settlement was announced by Benton J. Campbell, JD, U.S. attorney for the Eastern District of New York, and Gregory G. Katsas, JD, assistant attorney general for the Justice Department's Civil Division.

In addition, the hospital will pay the State of New York $14,883,883,

EXECUTIVE SUMMARY

A New York hospital is paying $89 million to settle lawsuits filed under the False Claims Act and to reimburse the state for improper billing. Analysts say the huge settlement should be a warning to risk managers that intense scrutiny of billing and coding is necessary to prevent such a financial disaster.

- A government investigation concluded that the hospital knowingly used incorrect billing codes for cancer treatment performed at the hospital.
- The whistle-blowers will receive millions for revealing the alleged fraud.
- Risk managers must be ready to respond quickly with a full investigation.

representing damages sustained by the state's Medicaid program. In total, SIUH will pay $88,916,448.

The biggest lesson from the case is that state governments are now going to be much more involved in FCA prosecutions, says **Christopher DeMeo**, JD, an attorney with the law firm of McGlinchey Stafford PLLC in Houston. That is partly the result of an incentive program the federal government instituted in 2007 that encourages states to enact their own FCAs to piggyback on the federal law, he explains. When properly constructed, the state law will provide the state with 10% more of any recovery from Medicaid fraud than the state would otherwise receive.

The new state incentive could be particularly dangerous for hospitals or nursing homes that have a large Medicaid population, he says.

"This is the proverbial sleeping dog that's been kicked. Now you have to watch out for it," DeMeo says. "With state budgets being squeezed and the potential for big revenue from the False Claims Act, you're going to see this kind of thing being litigated a lot more. This is the sign of things to come, as states have more financial incentive to become involved, and they become more aggressive in rooting these things out."

DeMeo notes that in Texas, the state attorney general's office has shown more interest lately in increasing funding and staff to investigate fraud and abuse in the Medicaid program.

"The False Claims Act had plenty of power before, but it was only the Justice Department that came after you, and they had a limited number of U.S. attorneys who could focus on fraud," DeMeo reports. "Now, you've essentially doubled that law enforcement potential by adding the states."

So far, 13 states have passed their own FCAs, and other states are in the process of doing so, DeMeo says. **(See p. 125 for a rundown of the states.)**

Corporate integrity agreement, also

The SIUH settlement, in part, resolves suits filed on behalf of the government in the U.S. District Court for the Eastern District of New York by two individuals, Campbell says. **(See p. 124 for details on the lawsuits.)** He says risk managers should beware falling prey to similar actions.

"Those who defraud and jeopardize the nation's vital, federally funded health care programs will be aggressively investigated and held to account," Campbell says. "Only by ensuring that the billing and cost guidelines of Medicare and Medicaid are scrupulously followed can we have confidence that affordable healthcare will continue to be available for those in need."

Katsas says the resolution of these claims against SIUH "demonstrates the federal government's continuing commitment to protect federally funded health care programs from any and all attempts by those who would knowingly seek improper payments."

HHS Inspector General **Daniel R. Levinson** notes that, in addition to the financial payout, SIUH has agreed to enter into a Corporate

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

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

Subscriber Information

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

Subscription rates: U.S.A., one year (12 issues), $495. Add $17.95 for shipping & handling. Outside U.S., add $30 per year, total prepaid in U.S. funds. For approximately 15 CE nursing contact hours, $545. Discounts are available for group subscriptions, multiple copies, site-licenses or electronic distribution. For pricing information, call Tria Kreutzer at 404-262-5482. Missing issues will be fulfilled by customer service free of charge when contacted within one month of the missing issue date. **Back issues**, when available, are $87 each. (GST registration number R128870672.)

AHC Media LLC is accredited as a provider of continuing nursing education by the American Nurses Credentialing Center's Commission on Accreditation.

This activity has been approved for 15 nursing contact hours using a 60-minute contact hour.

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

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

Healthcare Risk Management® is intended for risk managers, health system administrators, and health care legal counsel.

Opinions expressed are not necessarily those of this publication. Mention of products or services does not constitute endorsement. Clinical, legal, tax, and other comments are offered for general guidance only; professional counsel should be sought for specific situations.

Editor: **Greg Freeman**, (770) 998-8455.
Editorial Group Head **Russ Underwood** (404) 262-5521 (russ.underwood@ahcmedia.com).
Managing Editor: **Karen Young** (404) 262-5423 (karen.young@ahcmedia.com).
Senior Production Editor: **Nancy McCreary**.

Editorial Questions

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

Integrity Agreement with the Office of Inspector General, Department of Health and Human Services (OIG-HHS) under which the hospital will maintain a compliance program to help ensure against a recurrence of fraud.

"Settlements such as this demonstrate yet again that submitting fraudulent claims to Medicare and Medicaid artificially raises health care costs and in turn steals from those who depend on these government medical programs," he says. "The Office of Inspector General, working with our federal and state law enforcement partners, will continue to aggressively investigate and prosecute such fraud."

Malpractice case could evolve to qui tam

Because the payouts are the result of a negotiated settlement rather than a court ruling, there are no bright lines defined by the case, no clear indications that certain actions are legally permissible or impermissible, DeMeo says. But, he says, risk managers still can read between the lines and glean lessons in how to avoid similar trouble.

"It's clear that some of the things that were alleged in this case should not happen at any hospital. Like having a secret, locked ward of detox for alcohol and substance abuse that was deliberately hidden from state investigators, so they wouldn't have to fulfill licensing requirements and could still bill Medicaid," he says. "That is something that was wrong before, is wrong now, and is going to be wrong in the future."

DeMeo also points out that one of the *qui tam* lawsuits arose from a medical malpractice claim, so he says risk managers always should consider that possibility when dealing with patient and family complaints.

"Even if that complaint doesn't have merit as a malpractice claim, it could lead to an investigation or a lawsuit by an individual. It doesn't have to be the government that files the lawsuit against you," he says. "When the individual files a *qui tam* suit, it hits the hospital a lot harder than the malpractice would have. There's more money involved potentially, and it might not be covered by insurance."

In addition, DeMeo says, attorneys will be motivated to use the FCA in addition to or instead of pursuing the malpractice case that started the ball rolling. For one thing, attorneys' fees can be recovered with an FCA case, whereas they typically cannot be in a malpractice case.

"With this news coming out, I think a lot of lawyers who have malpractice cases pending are going to include things in their discovery requests to see if there are any types of Medicaid violations that they can hook onto," he says. "They will be looking to either increase pressure for settling the malpractice claim, or they will be hoping to increase their recovery."

Lack of documentation at fault?

One attorney points out that SIUH may have created some of its problems, or made them worse, by failing to document medical care carefully. **Russell Hayman**, JD, head of the health department in the Los Angeles office of the law firm McDermott Will, currently represents a number of health care providers under active criminal and civil investigation by OIG-HHS, the U.S. Department of Justice, and various U.S. Attorneys' Offices. The SIUH case involved essentially three allegations, he says. The lawsuits asserted that the hospital provided care in unlicensed beds, miscoded uncovered cancer therapies as covered therapies in order to obtain payment, and claimed an inflated number of medical residents in order to obtain graduate medical education expenses.

Hayman notes that the allegation concerning miscoded cancer therapy could have been a documentation problem.

"The therapy provided might not have been covered, or it might not have been reimbursable because it was not adequately documented. We can't tell from the news reports," he says. "Many of these types of cases involve lack of documentation. Better training in documentation and monitoring can catch a lot of those problems."

The unlicensed beds and inflated residency counts could have some explanation as well, Hayman says. Perhaps some beds were taken out of licensure or the size of the residency program was reduced, he says. Residents also could have been sent on more residency rotations.

"So it could be that the residency data that was reported to Medicare was not accurately changed to reflect those evolving facts," he says. "The failure to change the data and make sure what was being reported was accurate and current could result in overclaiming reimbursement in those programs."

If something like that happened at SIUH, that could show that the excess claims were more the result of carelessness than a conspiracy to defraud the government, but Hayman says in the end that will be just a footnote, because prosecutors still won't be forgiving if you ended up with too much

SOURCES

For more information on the False Claims Act, contact:

- **Christopher DeMeo**, JD, McGlinchey Stafford PLLC, Houston. Telephone: (713) 335-2132. E-mail: cdemeo@mcglinchey.com.
- **Russell Hayman**, JD, McDermott Will & Emery, Los Angeles. Telephone: (310) 551-9334. E-mail: rhayman@mwe.com.
- **Brian D. Roark**, JD, Bass, Berry and Sims, Nashville, TN. Telephone: (615) 742-7753. E-mail: broark@bassberry.com.

state and federal money. The lesson for risk managers, Hayman says, is that virtually any change in a hospital's operations requires reassessing the data that are used for reimbursement. Any time you start or end a program, expand or downsize anything, even remodel a facility, those changes must be reflected in what you submit to the government — promptly.

Resolve problems quickly, before they grow

Brian D. Roark, JD, an attorney with the law firm of Bass Berry in Nashville, TN, says the SIUH settlement is significant due to its size, which makes it one of the largest settlements ever by a single health care institution.

"Additionally, the settlement is of note in that it follows on the heels of a $76.5 million settlement by the hospital in 2005 relating to clinic services and a $45 million settlement in 1999 relating to therapy services," he reports.

Roark notes that the huge settlement came from two unrelated *qui tam* lawsuits, as well as additional unrelated violations that had been self-disclosed by the hospital. The hospital had a lot going wrong and apparently did not respond aggressively enough at the first signs of trouble, he says.

"The settlement highlights the importance to organizations of, when possible, resolving allegations of misconduct in one fell swoop to promote closure, allow the organization to move forward with its business, reduce legal expenses, and avoid return visits from the government," he says.

The lesson, Roark says, is that risk managers must be ready to move quickly when trouble arises. Don't freeze up. Don't panic. Don't wait until things get so bad that you can't fight the momentum of *qui tam* lawsuits and multiple government investigations.

"When an organization learns of alleged fraudulent conduct, whether through an internal audit report, an employee hotline call, or a subpoena from the government, it is of utmost importance for the organization to conduct a thorough investigation of sufficient scope to discover any instances of wrongdoing and then to respond appropriately," he says.

Hayman also points out that it is important for a health provider to have a culture in which employees are willing to come forward and report fraud, or at least their concerns, without fear of retribution. Otherwise, those same people may pursue FCA lawsuits instead.

DeMeo agrees that the SIUH case must be a wake-up call for risk managers. Expect more scrutiny of Medicaid claims, and remember that your state FCA may be even more strict than federal rules. With more prosecutors looking for fraud, risk managers may need to reassess their priorities.

"Whereas maybe some tasks may not have merited the effort in an overtaxed system, now you have to look at that in light of there being more publicity and more oversight by more authorities," DeMeo says. "The stakes just got higher." ■

Widow, doctor blew whistle on SIUH

The $89 million settlement by Staten Island University Hospital (SIUH) was prompted when two people — one the widow of a cancer patient and the other a doctor who saw improper billing — sounded the alarm through lawsuits filed under the False Claims Act (FCA).

Elizabeth M. Ryan, widow of an SIUH cancer patient, asserted in her federal FCA suit that SIUH fraudulently billed Medicare for stereotactic body radiosurgery treatment that was provided on an outpatient basis to cancer patients. She originally pursued a malpractice claim, but then filed a *qui tam* lawsuit when questions arose about billing for the treatment. The investigation established that from 1996 through 2004, SIUH defrauded Medicare and TRICARE by knowingly using incorrect billing codes for cancer treatment performed at the hospital. By using incorrect codes, SIUH obtained reimbursement for treatment that was not covered by Medicare or TRICARE. SIUH will pay the United States $25,022,766 to settle the claim, according to

States that have enacted False Claims Acts

Of the 13 state laws creating their own False Claims Acts (FCAs), some have been approved by the federal government and some have not. Approval means the states can receive 10% more of the recovery from a federal FCA case than they would receive if they had no state FCA, explains **Christopher DeMeo**, JD, an attorney with the law firm of McGlinchey Stafford PLLC in Houston.

Even if the state FCA does not meet the federal Office of the Inspector General (OIG) requirements for, however, it still is a valid law that can be enforced by the state. Given the financial incentive to comply with the OIG's requirements, most of the noncompliant laws will likely be redrafted, DeMeo says. Many more states are in the process of enacting their own acts.

These states have created FCA laws that meet the OIG requirements:

- California
- Georgia
- Hawaii
- Illinois
- Indiana
- New York
- Rhode Island
- Tennessee
- Texas
- Virginia

These states have laws that currently do not comply with the federal criteria:

- Florida
- Louisiana
- Oklahoma

an agreement that has been approved by U.S. District Judge John Gleeson, JD.

Miguel Tirado, MD, a former SIUH director of Chemical Dependency Services, who filed suit under the federal FCA and the New York State FCA, alleged that the hospital had fraudulently billed Medicaid and Medicare for inpatient alcohol and substance abuse detoxification treatment. The government's investigation established that, during the period July 1, 1994, through June 30, 2000, SIUH submitted claims for payment for detoxification treatment provided to patients in beds for which SIUH had received no certificate of operation from the New York State Office of Alcoholism and Substance Abuse Services (OASAS).

Although SIUH was authorized to provide inpatient detoxification care to patients in 56 beds, it administered treatment in 12 additional beds located in a locked, separate wing and concealed the existence of the wing from OASAS, according to the Justice Department. SIUH has agreed to pay the United States $11,824,056 and $14,883,883 to the state of New York according to an agreement that has been approved by U.S. District Judge Edward R. Korman, JD. New York State's claim was litigated by the New York State Attorney General's Office, Medicaid Fraud Control Unit.

The settlement also concerns SIUH's billings to Medicare and Medicaid for treatment of psychiatric patients in unlicensed beds during the period of July 2003 through September 2005. The hospital has agreed to pay the United States $1,478,989 to settle this claim.

The federal FCA and newly enacted New York state FCA permit private individuals to file suits on behalf of the government and receive a portion of the recovery.

As a result of the settlement, Tirado will receive $2.3 million from the federal government and $2.97 million from New York. Ryan will receive $3.75 million as her portion of the federal recovery.

The government's other two claims were resolved prior to the filing of suit. The United States had determined that SIUH deliberately inflated its resident count from the 1996 cost report year through the 2003 cost report year. Medicare pays a share of the cost of Graduate Medical Education at teaching hospitals such as SIUH. The amount paid is determined by Medicare annually based upon "cost reports" submitted by the hospitals. SIUH has agreed to pay the United States $35,706,754 to settle this claim. ■

Disruptive doctors must know they can get help

(Editor's note: This is the second of a two-part series on disruptive physicians. The October 2008 issue of Healthcare Risk Management *discussed how this behavior can threaten patient safety and lead to liability. This month's article provides more advice on how to deal with those professionals.)*

Dealing with disruptive physicians is no easy task, even if you recognize the importance of preventing their bullying, abusive behavior. Creating a culture in which such interaction is not

EXECUTIVE SUMMARY

Responding to disruptive behavior requires a multifaceted approach that combines prevention with an effective response to incidents. Early intervention with individual physicians can nip the problem in the bud.

- Query staff and physicians to determine how much the problem affects your organization.
- Address the stressful conditions that can lead physicians to act out inappropriately.
- Look for options other than suspending privileges.

tolerated is a good step, but you also must be willing to get physicians help when they need it.

In a recent alert to health care providers, The Joint Commission warned that disruptive physicians can threaten patient safety and announced new standards requiring health care organizations to create a code of conduct that defines acceptable and unacceptable behaviors and establishes a formal process for managing unacceptable behavior. The new standards take effect Jan. 1, 2009, for hospitals, nursing homes, home health agencies, laboratories, ambulatory care facilities, and behavioral health care facilities across the United States. *(Editor's note: For the full* Sentinel Event Alert, *go to http://www.jointcommission.org/SentinelEvents/SentinelEventAlert/sea_40.htm.)*

Risk managers are unlikely to know just how much disruptive physicians are affecting their organizations unless they make a concerted effort to ask those who are affected, says **David Maxfield**, a consultant in Provo, UT, who has studied communication issues in health care and co-authored the book *Influencer: The Power to Change Anything* (McGraw-Hill; 2007). He says one of the first steps in addressing the issue is to solicit input from the affected parties. Maxfield recently worked with a hospital administrator who sent an e-mail requesting reports about disruptive behavior, hoping to get a half-dozen that might give her some sense of what type of incidents were occurring.

"She got 12 replies in the first day, and then they started pouring in," Maxfield says. "People were walking up to her crying, saying they hadn't told anyone because they didn't think anyone cared."

Maxfield cautions that you must avoid letting physicians feel besieged when the institution starts addressing disruptive behavior. He recalls working with one hospital that was implementing a physician code of conduct, starting in the operating room, when the doctors started to complain that they were being cast as the bad guys. They also felt that the code of conduct was one more in a long series of demands and ultimatums put before them.

"They suggested that, at the same time, we also look at the conditions and behaviors that led physicians to flip out and act in unacceptable ways," he says. "What they found was that, a lot of times, the physician wasn't reacting to any one single incident, but because whatever was happening was part of a longstanding pattern. Once the hospital was willing to say they wanted to address those problems and lower the stress levels, they found more acceptance from the physicians."

Some problems years in making

Disruptive physicians often have a pattern of such behavior that goes back for years, sometimes decades, says **Michael Williams**, PhD, a principal with the Professional Renewal Center in Lawrence, KS, which treats physicians whose careers are in jeopardy because of disruptive behavior. An early intervention with those doctors could prevent an ongoing problem that gives the physician a bad reputation among peers and staff, which then makes all interaction more difficult, he says.

Streamlining response procedures can help, Williams says. In too many cases, he says, health care organizations must follow such a long, complicated procedure with a series of committees and hearings that it is years between the incident and any resolution. That isn't fair to the physician, and it doesn't do much to improve staff perception either, he points out.

Medical bylaws should provide for some type of disciplinary action short of suspension, Williams suggests.

"Bylaws often only allow you to suspend the doctor's privileges when the offense is significant enough and, of course, organizations are often loathe to do that," he says. "When you have something available that is less than a suspension, then you are more likely to use that option and be able to shape the behavior. Otherwise, the only option is a nuclear option, which can be good for ending behavior but not shaping it."

Any risk manager interested in addressing disruptive behavior must commit to a broad effort that encompasses prevention, immediate intervention, and then post-event analysis, says **Alan H. Rosenstein**, MD, MBA, vice president and medical director of VHA West Coast in Pleasanton, CA,

SOURCES

For more information on disruptive physicians, contact:

- **David Maxfield**, Author, Provo, UT. Telephone: (801) 724-6334. E-mail: dmaxfield@vitalsmarts.com.
- **Alan H. Rosenstein**, MD, MBA, Vice President and Medical Director, VHA West Coast, Pleasanton, CA. Telephone: (925) 730-3003. E-mail: arosenst@vha.com.
- **Michael Williams**, PhD, Principal, Professional Renewal Center, Lawrence, KS. Telephone: (785) 842-9772. E-mail: mwilliams@prckansas.org.

who has conducted extensive research on the topic and spearheaded his health care system's response. Rosenstein's research with VHA facilities and staff was part of The Joint Commission's basis for issuing the recent call to action.[1]

"This is not an issue where you can just say you're going to prevent it from happening or you're going to respond after the fact," he says. "You should try to prevent it from happening; but in reality, there still will be some events and you have to be ready to respond appropriately."

The goals of any action plan should be to prevent the events from occurring, but also respond to the events in real time — not days or weeks later. That quick response is essential to keeping disruptive behavior from harming patients or staff, Rosenstein says. Then after the event is addressed in real time, there must be a follow-up later to review what happened.

To implement any plan, Rosenstein says, the risk manager should recruit a physician champion who can spearhead the effort with his or her colleagues. That will greatly increase the chances of success, he says.

Based on his work with VHA facilities that addressed the issue, Rosenstein offers this summary of some of the key steps he says can minimize the dangers of disruptive physicians:

1. Assess the frequency of disruptive behavior and the seriousness. One good method is a confidential survey of staff and physicians.

2. Understand what factors can prompt disruptive behavior. The stress of working in health care is one obvious catalyst, but many other factors may be at play, including race, ethnicity, and economic pressures. Assess what issues may be at play in your own facility and also between certain people.

3. Secure a commitment from top leadership in the organization and then publicize that commitment. Make sure everyone in the organization knows that your top leaders are behind this effort and will not tolerate disruptive behavior.

4. Establish clear policies and procedures, and then enforce a zero-tolerance policy for violations.

5. Encourage incident reporting and make it safe for staff to do so without retribution. Also have a system in which you quickly and consistently respond to those reporting disruptive behavior to assure them that the report is taken seriously and being investigated.

6. Facilitate discussion of the problem among staff and physicians. Offer forums in which people can talk freely. Lunch meetings are one option, but so are more formal avenues such as task forces and medical staff meetings.

7. Provide education and training for both physicians and staff. The first step is simply raising awareness about the problem, and then you can move on to more specific issues such as stress management, conflict management, and assertiveness training.

8. Help staff and physicians improve communication by providing appropriate training and resources. There are many options available, including crew resource management.

9. Have a methodology for intervening in disruptive behavior. Know what you will do when you get a report, be ready to respond, and apply this policy consistently. Some VHA facilities use a "Code White" call for assistance when disruptive behavior requires mediation. It also is important to have a procedure for immediately debriefing those involved to get a clear picture of what happened and how it might be prevented in the future.

Reference

1. Rosenstein AH, O'Daniel M. A survey of the impact of disruptive behaviors and communication defects on patient safety. *Jt Comm J Qual Patient Saf* 2008; 34:464-470. ■

Manage time with tips that some swear by

(Editor's note: This is the second of a two-part series on time management for risk managers. Last month's Healthcare Risk Management *looked at the need for good time management strategies. This month, we provide more tips on time management for risk managers.)*

The first key to better time management is to realize that the term actually is misleading, says **Barry Izsak**, a productivity expert in Austin, TX. You can't manage time, but you can manage yourself.

"We all have time to accomplish our priorities if we identify them and then manage ourselves," he says.

Planning can be a bugaboo for managers, Izsak says. Planning is good, of course, but he says risk managers can not do it enough, or they can overdo it. Planning helps you become proactive with your time if it is done correctly, rather than simply being reactive — running around putting out fires.

"At the end of the day, people should write down, while the day is fresh in their mind, the three big things you want to get done the next day," he says. "There still will be interruptions tomorrow and maybe you'll only accomplish one or two of those things on your list, but even then you're far ahead of the game, better off than if you just came to work the next morning and started reacting to each new event."

Remember that working longer rarely is the solution when you feel overburdened or behind in your work, Izsak says. Better organization and planning can help you accomplish more than simply staying late at the office, he says. Having specific goals for the day, the week, and the month can help you stay on track and get the important work done even if you are periodically interrupted and thrown off track.

"When people work 10, 12, and 14 hours a day, they are just spreading their inefficiency over a long time period," he says. "Focusing on those top things you want to do in the day are really key. Schedule them in your planner just like a doctor's appointment or a meeting with your colleagues. You make those things happen because you schedule them, and so you need to schedule your main goals, too, or they're not going to get done."

Sometimes you must "defend your calendar," says **Pamela Dodd**, PhD, productivity expert, Orlando, FL. That means sticking with your scheduled activities unless absolutely necessary to deviate, she says. That includes your personal and family time, which can be the most difficult to defend.

Dodd also recommends determining your own "peak time," the time of day when you are most efficient — early morning, for instance. If that is your best time, when you can really churn out great work in high volume, schedule your day accordingly so that interruptions are minimized. Block out that time for your most important or most challenging tasks and really dig in.

Find a way to focus

Drew Stevens, PhD, a productivity expert in St. Louis, also emphasizes that a clear focus on the most important goals is key to making progress.

"If you're just staring at this huge pile of work that needs to be done and the phone's ringing and three people want your attention, nothing will ever be accomplished. You'll be overwhelmed and just respond to whoever's yelling the loudest at that moment," he says. "It is crucial that you seize control of your time and protect it. Don't make it available to just anyone. Keep your eye on the big picture and apportion your most precious resource, time, wisely."

Stevens says there are four key steps to managing your time more effectively:

1. Do not procrastinate. It wastes time when you already have too little. Sometimes it helps to do the things you hate to do first and get them off of the plate.

2. Do little things first so that you can get to the large items and focus on them. It is easy to waste time thinking about the little items that are distracting you from the bigger tasks, when you could just do them and get them out of the way.

3. Prioritize your tasks. Do the things that are most important that day, and do not try to do more than you know is possible. It is better to accomplish your most important tasks than to have done a little bit of work on everything.

4. Make a "don't-do" list. These are the things that interrupt or waste your time. The list will vary for each person, but they may include web surfing or listening to the radio, or letting a co-worker sit down in your office to chat.

EXECUTIVE SUMMARY

Improving your time management is all about changing the way you work. There is a limited amount of time in the day, so the solution lies in working more efficiently.

- Prioritize your tasks and focus on the most important.
- Schedule everything you need to do and then defend your calendar against interruptions.
- Organize your work so that you don't waste time looking for materials.

SOURCES

For more information on time management, contact:
- **Pamela Dodd**, PhD, Productivity Expert, Orlando, FL. Telephone: (407) 876-8189. E-mail: pamdodd@mindspring.com.
- **Barry Izsak**, Productivity Expert, Austin, TX. Telephone: (512) 419-7526. E-mail: barry@arrangingitall.com.
- **Drew J. Stevens**, PhD, Productivity Expert, St. Louis. Telephone: (877) 391-6821. E-mail: drew@gettingtothefinishline.com.

Organization can help you feel more in control and minimize the time spent tracking down information or trying to remember what you're supposed to be doing. Tickler files can be especially helpful for an overburdened manager, Dodd says. There are tons of things that you have to remember to do at a certain time or projects that you should check on periodically, so a tickler file can be a great way to make sure those things don't fall through the cracks, she says. Any calendar or electronic organizer will provide a way to plug in reminders, so be sure to fully utilize this option, she says.

Dodd also cautions about an overdependence on "organized piles." Sometimes even organized, neat people can become dependent on placing items in a pile here and another pile there, knowing all the time what the pile contains. But that just invites disaster, she says.

"Sooner or later, you're going to need something important, and you'll have to go tearing through those piles to find it. And you're probably the only one who has any idea what the piles are, so your assistant can't really help," she says. "Take the time to really organize and file things, even if it seems like another burden at the moment. You'll thank yourself later when you have to find that file in a hurry." ■

Safety team cuts birth trauma rates 93%

Any risk manager with hopes of reducing birth trauma rates should look to The Seton Family of Hospitals, based in Austin, TX, for lessons in what can yield dramatic results. The system, which includes eight hospitals in central Texas as well as other clinics, is seeing great success with an initiative to reduce preventable birth injuries.

The program resulted in a 93% reduction in birth trauma rates from 0.3% for 2001-2003 to 0.02% in 2006, says Seton President and CEO **Charles J. Barnett**.

"We were already at about half the national birth trauma rate, but we knew we needed to do better," he says. "Through the good work of our nurses and physicians, we've been able to reduce our rates even more. In fact, over the past year, we've experienced zero birth traumas, which is truly remarkable."

The Seton initiative began with the formation of the Perinatal Safety (PNS) team, a multidisciplinary workgroup, Barnett says. An analysis completed by both PNS and an intensive failure mode and effect analysis (FMEA) workgroup of physicians and nurses identified high-risk elements of the process. New protocols and policies were instituted, including no vacuum delivery prior to 36 weeks gestation, no combined usage of vacuum and forceps, and no elective induction prior to 39 weeks gestation.

In addition to reducing birth trauma rates, Seton decreased prematurity rates to 0.16% in 2004-2006 from 0.25% in 2001-2003; reduced instrumented delivery rate to 4.7% in 2004-2006 from 7.4% in 2001-2003; and reduced elective labor inductions prior to 39 weeks of gestational age to zero by October 2005, down from 3.2%.

The latest results from Seton show continuing improvement, says **Frank Mazza**, MD, a pulmonary and critical care physician with Seton who was a leader of the team to reduce birth trauma. Data recently published by Mazza and his colleagues show the rate of vacuum and forceps delivery at the end of 2007 was 4.1%. During

EXECUTIVE SUMMARY

A Texas hospital system has reduced birth trauma rates 93% by implementing a perinatal safety team. In addition, the system implemented new protocols and policies for deliveries.
- Vacuum delivery is prohibited prior to 36 weeks gestation.
- Elective induction is not allowed until 39 weeks gestation.
- The program also reduced prematurity rates.

SOURCES

For more information on the Seton effort to reduce birth trauma, contact:

- **Charles J. Barnett**, President and CEO, The Seton Family of Hospitals, Austin, TX. Telephone: (512) 324-7000. E-mail: Cbarnett@seton.org.
- **Frank Mazza**, MD, Pulmonary and Critical Care Physician, The Seton Family of Hospitals. Telephone: (512) 459-6599. E-mail: FMazza@seton.org.

the first three project years (fiscal years 2004 to 2006), the average length of stay for infants admitted to the neonatal intensive care unit for birth injury declined by 80% compared with the previous three years, from 15.8 to 3.1 days.

The effort began in October 2003, Mazza says. An interdisciplinary team from the four hospitals that provide obstetrical services met monthly to develop best practices to be used throughout the system. The team continues to meet monthly to share results and review the best practices.

Forceps and vacuum deliveries were an immediate focus because of the potential for causing birth trauma in an effort to speed the delivery. When the team implemented the protocols that sharply restrict the use of those two methods, it made clear that the rules were mandatory.

"We saw an immediate and dramatic drop in our birth trauma associated with assisted delivery," he says. "That impressed the physicians and staff, but it also empowered our team by showing us that we were on the right track."

The team then tackled another issue that can drive risk managers to distraction: the induction of babies before full term, which can greatly increase the risk of complications related to prematurity. Once the rule was implemented to prohibit inductions before 39 weeks, Seton saw a dramatic drop in prematurity. That led to a dramatic cost savings in the neonatal intensive care unit (NICU).

"We went from $4 million per year for babies that had iatrogenic prematurity, to $186,000, literally a 93% reduction in costs for taking care of these babies," Mazza says. "We did the right thing for the patient, but we killed the costs in that area, too. The risk managers loved it."

The Seton team then tackled other causes of birth trauma and got the number of incidents down to zero for about 15 months, even though the system does more than 10,000 deliveries a year. There were an average of 29 birth traumas per year in the Seton system before the project began, Mazza says.

"The efforts to reduce birth trauma also have resulted in a dramatic reduction in our insurance premiums," Mazza says. "So much risk is concentrated in the perinatal area, and achieving such dramatic drops in birth trauma can produce a significant, tangible result for the organization."

Reference

1. Mazza F, Kitchens J, Akin M, et al. The road to zero preventable birth injuries. *Jt Comm J Qual Patient Saf* 2008; 34:201-205. ■

'Never events' tied to one of six med-mal claims

Four recognized categories of hospital-acquired conditions, "never events" that have received more attention in recent years, make up 12.2% of total medical professional liability costs, according to the 2008 Hospital Professional Liability and Physician Liability Benchmark Analysis released recently by risk management services provider Aon Corp. and the American Society for Healthcare Risk Management (ASHRM), both in Chicago.

Hospital-acquired infections, hospital-acquired injuries, objects left in surgery, and pressure ulcers account for one out of every six claims, the report says.

On Oct. 1, the Centers for Medicare & Medicaid Services ended reimbursement for 10 specific hospital-acquired conditions — often referred to as "never events." The new research shows that never events are more than just a freak occurrence, says **Greg Larcher**, director and actuary of Aon Global Risk Consulting and author of the analysis. The study shows that they make up an alarming portion of medical malpractice cases.

COMING IN FUTURE MONTHS

- ■ Normalization of deviance
- ■ Wrist bands and privacy concerns
- ■ Health system cuts med errors 29%
- ■ Admitting convicted sex offenders

"The increased awareness surrounding these nonreimbursable conditions may cause a rise in the frequency of related hospital professional liability claims, not to mention other hospital-acquired conditions not currently addressed by CMS regulations," Larcher says. "This study marks the first time these conditions have been benchmarked, and provides a baseline moving forward for this essential piece of the liability picture."

The study also includes an analysis of professional liability costs for the surgery, obstetrics, and emergency departments. Various supplementary database segments appear in this year's analysis as well, including facility ownership, number of beds and teaching hospitals.

"For the fourth straight year, we are not seeing an increase in the overall number of liability claims," Larcher says. "That said, the not-for-profit segment of the database reflected an increase in claims for the second year."

More than 100 health care organizations representing more than 1,200 facilities, ranging from small community hospitals to large multistate publicly traded health care systems, provided loss and exposure data for the study. The hospital professional liability benchmark database includes 77,705 claims representing $9.3 billion of incurred losses. ■

Clarification

In the August 2008 issue of *Healthcare Risk Management*, the article "2009 safety goals address site marking," noted that an operative site should be marked by a licensed practitioner. The goal calls for the site to be marked by a licensed independent practitioner. We apologize for that error. ■

CE objectives

After reading this issue of *Healthcare Risk Management*, the CE participant should be able to:

- **Describe** legal, clinical, financial, and managerial issues pertinent to risk management in health care.
- **Explain** how these issues affect nurses, doctors, legal counsel, management, and patients.
- **Identify** solutions, including programs used by government agencies and hospitals, for hospital personnel to use in overcoming risk management challenges they encounter in daily practice. ■

CNE Questions

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

17. According to Christopher DeMeo, JD, what is the incentive program for states to enact their own False Claims Act?
A. The federal government requires it in order for state health providers to participate in Medicare.
B. When properly constructed, the state law will provide the state with 10% more of any recovery from Medicaid fraud than the state would otherwise receive.
C. The federal government increases Medicare reimbursement for all health providers when there is a state act.
D. Without a state act, the federal government reduces Medicare reimbursement for all health providers.

18. What does Alan H. Rosenstein, MD, MBA, say about disruptive behavior?
A. Risk managers should not try to reduce or eliminate disruptive behavior because that is the responsibility of the physician leaders.
B. With proper steps, it can be entirely eliminated.
C. It is not possible to even reduce disrupt behavior.
D. You should try to prevent it from happening, but in reality there still will be some events and you have to be ready to respond appropriately.

19. In the FCA settlement involving SIUH, what did the Justice Department conclude after investigating allegations by Miguel Tirado, MD?
A. SIUH submitted claims for payment for detoxification treatment provided to patients in beds for which SIUH had received no certificate of operation from the New York State OASAS.
B. SIUH had done nothing improper and Tirado's allegations were unfounded.
C. SIUH submitted claims for payment for detoxification treatment that were technically improper but which resulted in no reimbursement beyond what would have been appropriate anyway.
D. SIUH submitted claims for payment for detoxification based on an ambiguous federal rule that could be interpreted in different ways; therefore, the hospital was not responsible.

20. When The Seton Family of Hospitals System implemented protocols that sharply restrict the use of forceps and vacuum delivery, how were they described to physicians and staff?
A. The system made clear that the rules were mandatory.
B. The system made clear that the rules were voluntary.
C. The system made clear that the rules were required by government regulation.
D. The system made clear that the rules were required by the insurer.

Answers: 17. B; 18. D; 19. A; 20. A.

United States Postal Service
Statement of Ownership, Management, and Circulation

1. Publication Title	2. Publication No.	3. Filing Date
Healthcare Risk Management	1 0 8 1 – 6 5 3 4	10/01/08
4. Issue Frequency	5. Number of Issues Published Annually	6. Annual Subscription Price
Monthly	12	$495.00

7. Complete Mailing Address of Known Office of Publication *(Not Printer) (Street, city, county, state, and ZIP+4)*
3525 Piedmont Road, Bldg. 6, Ste. 400, Atlanta,
Fulton County, GA 30305
Contact Person: Robin Salet
Telephone: 404/262-5489

8. Complete Mailing Address of Headquarters or General Business Office of Publisher *(Not Printer)*
3525 Piedmont Road, Bldg. 6, Ste. 400, Atlanta, GA 30305

9. Full Names and Complete Mailing Addresses of Publisher, Editor, and Managing Editor *(Do Not Leave Blank)*
Publisher *(Name and Complete Mailing Address)*
Robert Mate, President and CEO
AHC Media LLC, 3525 Piedmont Road, Bldg. 6, Ste. 400, Atlanta, GA 30305

Editor *(Name and Complete Mailing Address)*
Joy Dickinson, same as above

Managing Editor *(Name and Complete Mailing Address)*
Coles McKagen, 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. If the publication is published by a nonprofit organization, give its name and address.)*

Full Name	Complete Mailing Address
AHC Media LLC	3525 Piedmont Road, Bldg. 6, Ste 400
	Atlanta, GA 30305

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
Thompson Publishing Group Inc.	805 15th Street, NW, 3rd Floor
	Washington, D.C. 20005

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**, September 1998 *See instructions on Reverse)*

13. Publication Name: Healthcare Risk Management
14. Issue Date for Circulation Data Below: September 2008

15. Extent and Nature of Circulation			Average No. of Copies Each Issue During Preceding 12 Months	Actual No. Copies of Single Issue Published Nearest to Filing Date
a. Total No. Copies *(Net Press Run)*			1250	1081
b. Paid and/or Requested Circulation	(1)	Paid/Requested Outside-County Mail Subscriptions Stated on Form 3541. *(Include advtertiser's proof and exchange copies)*	837	775
	(2)	Paid In-County Subscriptions *(Include advertiser's proof and exchange copies)*	6	0
	(3)	Sales Through Dealers and Carriers, Street Vendors, Counter Sales, and Other Non-USPS Paid Distribution	57	61
	(4)	Other Classes Mailed Through the USPS	21	53
c. Total Paid and/or Requested Circulation *(Sum of 15b(1) and 15b(2)*			921	889
d. Free Distribution by Mail *(Samples, Complimentary and Other Free)*	(1)	Outside-County as Stated on Form 3541	15	17
	(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)*			20	20
f. Total Free Distribution *(Sum of 15d and 15e)*			35	37
g. Total Distribution *(Sum of 15c and 15f)*			956	926
h. Copies Not Distributed			294	155
i. Total *(Sum of 15g. and h.*			1250	1081
Percent Paid and/or Requested Circulation *(15c divided by 15g times 100)*			96%	96%

16. Publication of Statement of Ownership
Publication required. Will be printed in the November 2008 issue of this publication. ☐ Publication not required.

17. Signature and Title of Editor, Publisher, Business Manager, or Owner: President and CEO — Date: 9/28/08

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 multiple damages and 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.
5. In item 16, indicate date of the issue in which this Statement of Ownership will be published.
6. Item 17 must be signed.

Failure to file or publish a statement of ownership may lead to suspension of second-class authorization.

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

Mishandling of fatal lung infection leads to $1.29M settlement in New York

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

News: A woman presented to the hospital complaining of left shoulder pain, chest pain, vomiting, and nausea. She was diagnosed with pneumonia and treated with IV antibiotics for two weeks, after which she was discharged. Two weeks later, the woman went to another hospital and was diagnosed with pneumonia and an abscess in her left lower lung. She was treated with IV antibiotics, but repeated recommendations for follow-up X-rays and CT scans were ignored for several days. When a CT scan was finally performed, it showed that the abscess had grown considerably. Doctors attempted to drain the abscess, but when they could not remove all the fluid, surgery was scheduled for the next day. The woman died that night, however, as a result of pneumonia and the lung infection. The woman's husband sued both hospitals and the various doctors for medical malpractice. After jury selection, but before opening statements, all the parties settled for a total of $1.29 million.

Background: A 50-year-old homemaker, who was 4-foot-11-inches tall and weighed 214 pounds, underwent bariatric surgery at a local hospital. Following the surgery, the woman vomited almost on a daily basis. She returned to the hospital three months later complaining of left shoulder pain, chest pain, vomiting, and nausea. She was admitted, and her history of vomiting was documented. She stayed at the hospital for two weeks, during which time X-rays and CT scans were taken, the results of which showed pneumonia, and she was treated with IV antibiotics. Upon her discharge, the woman was not given antibiotics or sent for follow-up care, despite the fact that her pneumonia had not resolved.

Two weeks later, the woman went to another hospital and was diagnosed with an abscess in her left lower lung and a cavitary mass resulting from aspiration pneumonia. A CT scan showed the abscess was 4.3 cm by 2.8 cm at the time of her admission. Her attending physician at the second hospital, an internist, called in an infectious diseases specialist and a pulmonologist, and over the next few days, the team of doctors continued to treat her with IV antibiotics. The woman's infection worsened, however, and the abscess continued to grow.

A week after her admission to the second hospital, the pulmonologist recommended that the woman undergo a follow-up chest X-ray, but the test was not performed. A couple of days later, the infectious diseases specialist evaluated the woman again and recommended that the woman be put on an additional antibiotic and that a follow-up CT scan be performed, but the attending physician did not carry out either of those recommendations. Six days after the pulmonologist first recommended that a follow-up chest X-ray be

ordered, the pulmonologist again recommended the test, and this time it was performed. It showed that the abscess had grown. That same day, the infectious diseases specialist again recommended a follow-up CT scan, as did a radiologist, but the scan was not performed.

The woman's condition continued to worsen, and the next day the pulmonologist performed a diagnostic bronchoscopy, which found nothing unusual except for the already-diagnosed pneumonia. The following day, a surgical consult was obtained, and a follow-up CT scan was suggested for now the third time. When the CT scan was finally performed the next day (six days after the infectious diseases specialist had originally recommended the procedure), it showed that the abscess had grown considerably. The doctors then decided to drain the abscess, which resulted in the removal of 40 cc of fluid. After discovering that no more fluid would drain, the woman's physicians decided that she should undergo surgery. The surgery was scheduled for the next day, but the woman died the night before as a result of pneumonia and the lung infection. The organism causing the infection was never diagnosed.

The woman was survived by her husband, a 10-year-old severely autistic son, and a 17-year-old daughter. The woman's husband, acting individually and on his wife's behalf, sued hospitals, the attending physician, surgeon, pulmonologist, and infectious diseases specialist. The plaintiff alleged that the doctors deviated from the accepted standards of medical care by failing to monitor, diagnose, and treat his wife's infection. He alleged that they failed to timely follow through with recommended CT scans and X-rays, which caused them to be unaware that his wife's abscess was increasing in size, and that the doctors should have realized that the first two antibiotics the woman was given were not effective, especially given the fact that she had a history of being in the hospital on antibiotics for two weeks prior to presenting to the second hospital. He contended that because of her prior treatment, the doctors should have known that there was a possibility of growing resistant organisms and that they therefore should have been more aggressive in her treatment. The husband also claimed the doctors should have recognized that the antibiotics were not effective and should have opted to drain the abscess or perform surgery earlier than they did. As for the hospitals, the plaintiff claimed that they were liable for the doctors' actions under agency principles.

The plaintiff sought recovery of damages for his wife's wrongful death and the pain and suffering she endured before she died, as well as loss of household services, to specifically include the fact that it was anticipated that she would have cared for her severely autistic son for the rest of her working life. The plaintiff also presented a derivative claim seeking to recover for loss of society and companionship.

The first hospital defended the suit by arguing that it initially thought the woman's complaints were orthopedic because she complained of left shoulder pain. It contended that it acknowledged that she had an infection and properly treated it with antibiotics, which it claimed resolved the problem. The first hospital argued that she had a normal white blood cell count when she presented to the hospital and that although it rose during her hospitalization, it had returned to normal by the time she was discharged.

The second hospital, the attending physician, and the pulmonologist defended the lawsuit by arguing that the woman was already very sick when she was admitted to the hospital. They claimed that the standard of care was medical management, i.e., treating the infection with IV antibiotics for 10 days to two weeks and monitoring the woman's condition before doing anything invasive. They argued that the woman appeared to respond to the antibiotics and that her illness plateaued during her three-week hospital stay. They further argued that the antibiotics she received were appropriate and that they did not add the third antibiotic as recommended by the infectious diseases specialist because it posed additional risks for the patient. Finally, they contended that there was no reason to do repeated radiologic studies because changes in the patient would be clinically apparent before they would be seen on X-rays or CT scans, and they argued that her treatment was followed step-by-step according to the standard of care.

The surgeon's defense was that the woman was stable at the time he was called and that there were no reasons to rush her to surgery prior to the next day. He contended that at the time he scheduled her for surgery, it was not an emergency.

The case proceeded to trial, but prior to jury selection, the first hospital agreed to pay the plaintiff a settlement of $550,000. After jury selection, but prior to opening statements, the remaining parties agreed to settle the case. The settlement included $390,000 from the second hospital (with an agreement to discontinue the case against the

attending physician), $325,000 from the pulmonologist, and $25,000 from the surgeon. The total settlement amounted to $1.29 million.

What this case means to you: "The first question is why the bariatric surgeon allowed her to go so long without some sort of intervention," says **Lynn Rosenblatt**, CRRN, LHRM, risk manager at HealthSouth Sea Pines Rehabilitation Hospital in Melbourne, FL. Three months out from surgery, she still was not medically stable, as daily nausea and vomiting is not normal even after a gastric reduction/bypass procedure. At her height and weight, she was morbidly obese and at very high risk for serious complications.

So, she now presents to the hospital and is diagnosed and treated for aspiration pneumonia. She has a significant past medical history and comorbid conditions. Her stay was given at two weeks, but there is no indication as to why she was there so long. Fourteen days is an extraordinary length of stay for pneumonia in today's managed care environment, which would suggest that her hospitalization was not a routine case of pneumonia.

No details are given as to any other testing than X-ray and CT scan, but there are facts presented that she was still very sick when she left the hospital. The fact that she was not scheduled for a follow-up appointment, at a minimum, to ascertain that her pneumonia had cleared and that her condition was significantly improved, indicates a violation of a commonly held standard of care.

If she had indeed improved after her release from the hospital, then no further treatment would have been necessary. But how was that to be evaluated without a post-discharge appointment? The attending physician managing her case was remiss in not scheduling her for another appointment after discharge and for not continuing some sort of antibiotic treatment given the apparent severity of the situation.

The failure to do so speaks to the possibility that the woman was being followed by a number of physicians, possibly employed by the hospital, who passed her off among themselves without discussing the case between them, so that all were unaware of the treatment being provided and what further treatment was necessary after discharge. Somehow, the continuity of the care plan was lost and the patient discharged without proper referral and prescription medications.

This is not an uncommon occurrence in hospitals, particularly where more than one physician is involved in the patient's care. This has prompted both The Joint Commission and the Centers for Medicare & Medicaid Services to impose a standard for "pass off." The standard specifically addresses the information that must be "passed off to the next level of care." The standard not only applies when a patient is discharged, but also when a patient is transferred between services within the hospital.

The standard provides greater assurance that the provider accepting responsibility for the patient's ongoing care — even on a short-term basis, as in the provision of a single procedure — is aware of what has transpired and what is planned for future care. In this case, the information would have been "passed off" to the patient and her husband at the time of discharge under the standard.

The nurse or individual acting as the discharging representative of the hospital should have reviewed the physician's orders for any ongoing medications and for any follow-up appointments at the time the patient actually left the acute care facility. The patient should have had any prescriptions reviewed to alert her and her husband to adverse side effects, any food interactions, and an appropriate administration schedule, including emphasis on taking the medication as prescribed. The discharging agent also should have reinforced the necessity of keeping all future appointments and advised the patient and her husband of any signs and symptoms of medical decline and what to expect in terms of recovery.

Obviously, this did not happen. The narrative does not detail what happened or who may have been following the case during the two weeks after discharge when the patient finally went to another hospital with her ongoing illness. What is evident, however, is that her condition was steadily worsening and that the pneumonia that had been previously diagnosed actually was the result of foreign matter in the lung from aspiration, which had resulted in an inflammatory abscess.

It is unclear why the pulmonologist waited so long before doing a bronchoscope as a more definite diagnostic tool. It is also unclear as to what caused the delay in obtaining the various studies as ordered by the attending physicians. Most hospitals have policies about currency of physician orders and how much lead time is required before a test must be scheduled and when it actually occurs. The pulmonologist who ordered the follow-up X-ray after the first week should have written for a stat or timed the order for an immediate film, as such would have assured that the

X-ray was prompt and timely.

Unfortunately, that did not occur and no one followed up on the delay. The standard of care that would apply to an ongoing hospitalization of a patient with this diagnosis and history was certainly breached, as the providers failed to provide ongoing supervision of care and interventions that were timely and appropriate to her presentation. The CT scan also was not performed as recommended, and the delay was unjustified because the patient's condition, as the X-ray showed, was clearly deteriorating.

Hospitals must have a system to assure that orders are processed in a timely manner and that the intentions of the physician are addressed in terms of scheduling and follow-through. The failure to monitor the timeliness of scheduling and the results of the procedure falls not only to the physician who wrote the order, but to the hospital staff tasked with assuring that it is done.

There also is no indication as to why the surgical consult was delayed for more than a week. Once the CT scan was completed, it was very evident that the patient's condition had been adversely affected by the delays in obtaining the recommended studies. Ultimately, the abscess was drained of a large quantity of fluid, and it is hard to believe that the patient was not having serious respiratory complications at that point.

Questions abound as to what were her symptoms, her blood laboratory findings, her vital signs — particularly oxygen saturation, temperature, and respiratory rate. Did nursing consistently document her ongoing condition, vital signs, any evidence of respiratory compromise, shortness of breath, patient's complaints, and her endurance? All would be evidence of either a stable or unstable situation, and it does not appear that, if these elements of care were actually being addressed, they were communicated to the physician staff as they should have been. It also raises the issue of how often the physicians rounded on their patients and what information they sought and/or verified with the nursing staff. Finally, the big question is, what the role of risk management or quality assurance in this misadventure?

It would appear that everyone with any responsibility for this patient failed to adhere to recognized standards of case management and medical oversight. The entire system of patient management apparently failed, and as a result this patient lost the opportunity for timely interventions that possibly would have spared her life.

The defense that was advanced by both of the hospitals and by the physicians was rather ridiculous given the situation and the time span that had elapsed from the onset of her situation to her death. Under accreditation standards, The Joint Commission requires a root-cause analysis, which is an in-depth review of the how, why and why not of a set of facts and exactly what went wrong at what juncture. In such a situation, with such dire consequences, such an investigation should have been done.

The most obvious indication that the situation was seriously deteriorating was the time frame where testing should have been completed and acted upon. Time and the failure of the providers to take action were clearly against this patient. Also, the patient was getting worse, but no one was acknowledging any responsibility for communicating with each other as to what needed to be done next and when it needed to be completed.

The case did settle but very close to trial. There is no indication of any attempt on the part of the various providers or their insurance companies to arbitrate or mediate the facts. Had that been done, perhaps the cost of trial preparation could have been avoided and a more equitable settlement may have been possible. The only positive outcome was that the defendants collectively came to their senses and realized that a jury verdict would unquestionably be higher and eventually settled before their dirty laundry could be aired in public.

Reference

- Case No. 27093/04; 14793/05, Queens County (NY) District Court. ■

HIPAA Regulatory Alert

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

Threat modeling to protect patient information

You can't afford not to

A health care organization might have in place the best information technology (IT) protections available, but complacency can be a dangerous thing considering the gold mine of personal information stored by a hospital.

Consider this: One Atlanta-based security services provider says it's blocking an average of 15,543 attempted hacker attacks a day per health care client, compared to an average 1,581 attacks per day per bank client.

To thwart an information thief, and thus comply with HIPAA requirements to protect personal health information, SecureWorks information security expert **Jon Ramsey** suggests thinking like an information thief.

"Sit your two best IT guys down for a while, and ask them how they'd break into your system, where they'd [attempt access], what they'd look for, and you'll come up with a pretty good threat model pretty quickly," Ramsey says. "Threat modeling means considering who is going to attack you, how, and what are the assets they're going to go after," says Ramsey.

Threat modeling has proved its value for a long time in the banking industry, and now is doing the same work in health care.

Threat modeling an ongoing process

While it would be nice to construct a mathematically precise threat matrix that, once put into place, would serve as a permanent threat model, in real life, threats change daily, so preemptive measures against those strikes have to change daily, too, Ramsey says.

Implementing HIPAA includes preventing privacy breaches and reacting to ones that occur, and since technology changes with each day — and hackers' knowledge broadens at the same pace — staying ahead means constant vigilance to anticipate potential problems.

When threat modeling for potential privacy vulnerabilities, health care organizations should consider some general questions:

- What's the nature of potential threats? (Are disclosures likely to be made accidentally, or is information likely to be stolen for profit, or both?)
- Who is the source of the threat? (Employees, visitors, vendors, outsider gaining access illegally.)
- How might access be gained? (Hacking into a computer, stealing a laptop, breaking into an office.)
- What data are vulnerable?
- How many data are vulnerable?

And now is a good time to think "threat model," as the stakes recently increased. The Department of Health and Human Services (HHS) sent a clear signal earlier this year that it takes the safeguarding of patients' personal information very seriously when it took enforcement action against Seattle's Providence Health & Services over the theft or loss of health information of more than 386,000 patients. **(See "HHS fines health system for breach of privacy," p. 2.)**

Patient information compromised

Providence's patient information was compromised because electronic media, such as backup tapes and laptops that contained unencrypted information, were left unattended and eventually lost or stolen. While HHS has received more than 6,700 reports of breaches under HIPAA, the Providence case was the first time HHS imposed a fine ($100,000) for a data breach, and industry observers have written that it signals more to come.

Because "you can't protect everything from everyone," Ramsey points out, no security plan can monitor every single bit of data and every

access point to those data; so it makes sense to put your greatest efforts toward the greatest risk.

In other words, he added (quoting former National Security Advisor McGeorge Bundy), "If you guard your toothbrushes and diamonds with equal zeal, you'll probably lose fewer toothbrushes and more diamonds."

Threat modeling allows a health care organization to take its limited IT and security budgets and use them to the greatest effect by narrowing down the areas of greatest vulnerability.

"You want to spend each dollar in a way that will make it more expensive for a threat to access your information," Ramsey adds.

Providers' need for quick access adds risk

Coupled with the attractiveness (to hackers) of the tremendous amount of personal identification data that's available from a health care patient record system is the vulnerability that's inherent when that information has to be readily and quickly accessible by those who legitimately need it — physicians, nurses, account managers, etc.

"It's the ubiquity of information; if you're an emergency room doctor and you need a patient's record, you get it right away," Ramsey says. Making that information easily administered and, at the same time, secure is why the field of IT in the health care setting has exploded in the last two decades.

"It's an organic thing; the threats change every day, so our clients have new threat models every day," Ramsey says. "What you need to say is, 'If I'm secure today and not tomorrow, what has changed?' and you have to ask yourself that every day."

With each new technology, there are new vulnerabilities; those multiply when you consider how many data systems within a hospital integrate or "map" to one another.

"The ubiquity of information and the need to integrate data across these systems leaves a lot of openness," Ramsey cautions.

And health care's use of existing technology is a boon to the "business" of information theft.

For example, Microsoft Windows has been around for 25 years, giving hackers a generation of time to learn its capabilities and vulnerabilities; now that the operating system is used in health care, "criminals have whole new business models to invade," Ramsey points out.

"We know from industries more advanced [than health care] in information security that threat modeling makes a whole bunch of sense," he concludes. "It's proven itself in other industries — you can't not do it."

[For more information, contact:

*• **Jon Ramsey**, Chief Technology Officer, SecureWorks, Atlanta. Phone (877) 905-6661.*

*• **Department of Health and Human Services.** Resolution agreement between HHS and Providence Health & Services; available online at http://www.hhs.gov/ocr/privacy/enforcement/resolution.html.]* ■

HHS fines health system for breach of privacy

On July 15, 2008, the Department of Health and Human Services (HHS) entered into an agreement with Seattle-based Providence Health & Services to settle potential violations of HIPAA privacy rules.

Under the agreement — the first time HHS has levied a fine for a data breach — Providence agrees to pay $100,000 and implement a detailed corrective action plan (CAP) to ensure that it will safeguard identifiable electronic patient information against theft or loss. Providence's data breach resulted from electronic record backups and laptop computers being left unattended, eventually leading to their loss or theft.

HHS says the breaches occurred when the backups and laptops were removed from Providence premises (in Oregon and Washington) and left unsecured; some thefts occurred when the items were left in Providence employees' cars.

While HIPAA does not specifically address transportation of personal health information via laptop (or car), the rule does require covered entities to safeguard portable media or devices, including paper charts being moved between offices.

Remediation steps taken

Under the resolution agreement — also the first HHS has required from a covered entity — Providence agrees to take remediation steps, including:

- Revising its policies and procedures regarding physical and technical safeguards (e.g., encryption);
- Governing off-site transport and storage of electronic media containing patient information, subject to HHS approval;

• Training work force members on the safeguards;

• Conducting audits and site visits of facilities.

According to HHS, it has received more than 30 complaints related to the loss or theft of patient information from Providence's data systems. The resolution agreement alleges that protected information of more than 386,000 patients was exposed by the breach.

(Editor's note: To read HHS guidance on HIPAA's security rule pertaining to electronic devices, go to www.cms.hhs.gov/ SecurityStandard/Downloads/ SecurityGuidanceforRemoteUseFinal122806.pdf.) ■

HHS guidance emphasizes what *can* be divulged

The Department of Health and Human Services (HHS) has issued new guidance for providers on talking about patients' health information with and in the presence of other parties — with an emphasis on what *can* be discussed.

Even though HIPAA requires health care providers to protect patient privacy, providers are permitted, in most circumstances, to communicate with the patient's family, friends, or others involved in their care or payment for care.

The guidance is intended to clarify HIPAA privacy requirements so that health care providers don't unnecessarily withhold information from those who are permitted to have it.

Examples of permitted discussions

Among examples discussed in "A Health Care Provider's Guide to the HIPAA Privacy Rule: Communicating with a Patient's Family, Friends, or Others Involved in the Patient's Care," released in September 2008 by the HHS Office of Civil Rights, are the following examples of permitted discussions of health information:

• An emergency department doctor may discuss a patient's treatment in front of the patient's friend if the patient asks that her friend come into the treatment room.

• A doctor's office may discuss a patient's bill with the patient's adult daughter who is with the patient at the patient's medical appointment and has questions about the charges.

• A doctor may discuss the drugs a patient needs to take with the patient's health aide who has accompanied the patient to a medical appointment.

• A doctor may give information about a patient's mobility limitations to the patient's sister who is driving the patient home from the hospital.

• A nurse may discuss a patient's health status with the patient's brother if she informs the patient she is going to do so and the patient does not object.

(Editor's note: "A Health Care Provider's Guide to the HIPAA Privacy Rule" is available free for download at www.hhs.gov/ocr/hipaa/provider_ffg.pdf.) ■

Privacy hindered by not-so-private hospital rooms

Despite increasing demand for privacy surrounding health information, North American hospitals lag behind European counterparts when it comes to one of the most visible impediments to privacy — multibed hospital rooms.

"Considerable attention is paid to the privacy of health information, yet multibed rooms do not provide such privacy," wrote the authors of a recent paper published in the *Journal of the American Medical Association.*[1]

According to **Michael E. Detsky**, MD, and **Edward Etchells**, MD, both of the University of Toronto, single-bed hospital rooms were recognized as the ideal setting for patient care early in the last century; however, while patient safety, dignity, and privacy have gained attention in hospital medicine, multibed rooms have remained.

Besides providing privacy, the authors suggest, single-patient rooms inhibit the spread of nosocomial infection and reduce the need for in-hospital transfers; on the other hand, they point out, one patient per room means more walking and time for hospital staff, and new construction costs are inherent in converting from multipatient rooms to single-patient rooms.

Nonetheless, the privacy protection afforded by a private room is demanded by a health care system that prizes patient privacy.

"Patients may not share sensitive medical history, such as sexual practices or illicit drug use, in a room where strangers can listen," Detsky and Etchells wrote. "Discussions about life-sustaining treatment or a serious diagnosis with a poor prognosis are inappropriate with other parties present

when separated only by curtains."

While North American hospitals lag behind, for example, in French hospitals, which have designed single-patient rooms as standard for hospitals for the last 20 years, single-patient rooms are becoming standard in new construction of medical/surgical wards and obstetrical units.

"Single-patient rooms are permanent physical features that potentially could improve safety and patient satisfaction without the need for ongoing staff training, audits, or reminders," the authors conclude.

Reference

1. Detsky ME, Etchells E. Single-patient rooms for safe patient-centered hospitals. *JAMA* 2008;300:954-956. ■

HHS lacking in approach to health info privacy

The Department of Health and Human Services (HHS) may have given rise to — and oversees — HIPAA privacy regulations, but according to a report by the General Accounting Office (GAO), the agency's approach to ensuring the privacy of health information still needs some work.

A report released in September 2008 by the GAO is a follow-up to recommendations made by GAO in 2007 on the status of efforts by HHS to ensure the privacy of personal health information exchanged within a health information network. At the time of the 2007 report, the GAO recommended that HHS define and implement an overall privacy approach for protecting information that's exchanged or stored electronically.

The GAO reported in its follow-up that HHS has taken steps toward meeting the recommendations, including identifying goals, ensuring key privacy principles are addressed, and addressing challenges associated with nationwide exchange of health information.

Still, while the GAO report credits HHS with taking steps that "contribute to an overall privacy approach," it finds HHS has fallen short of implementation; in particular, the report finds that HHS's privacy approach doesn't include a defined process for assessing and prioritizing privacy initiatives, causing gaps in policies and guidance needed by stakeholders to ensure adequate privacy protection measures.

The recommendation of the GAO is that HHS needs to prioritize; it suggests that HHS ask the national coordinator for health IT to include in the HHS overall privacy approach a process for assessing and prioritizing its privacy-related initiatives. ■

New rule would update rules for *e*transmissions

On Aug. 22, 2008, the Department of Health and Human Services (HHS) published a proposed rule that would adopt updated versions of the standards for electronic transactions under HIPAA. The rule also would adopt a transaction standard for Medicaid pharmacy subrogation and two standards for billing retail pharmacy supplies and professional services, and would clarify who the "senders" and "receivers" are in the descriptions of certain transactions. Comments on the proposed rule closed in October.

Updated versions of current HIPAA electronic transaction standards require the use of the ICD-10 code sets for claims, remittance advice, eligibility inquiries, referral authorization, and other widely used transactions. The proposed version, version 5010, adds the ability to designate certain information as confidential and restrict access to member information. This new function provides privacy protection by safeguarding confidential information, according to HHS.

Health care stakeholders, including the American Hospital Association and Blue Cross/Blue Shield, have asked HHS to forestall requiring implementation of ICD-10 until HIPAA electronic transaction standards have been modified to keep up with the massive coding changes.

"Before the transition to ICD-10 can begin, the industry must move to the next generation of HIPAA transactions [Version 5010] because the current version [4010] will not work with ICD-10," Blue Cross/Blue Shield stated in response to the proposal. "Version 5010 is a major rewrite of the HIPAA transaction standards, with more than 850 individual changes. There is wide industry consensus . . . that upgrading to version 5010 is too significant to be done in conjunction with ICD-10."

The ICD-10 changes are scheduled to become effective Oct. 1, 2011. To read the entire proposed rule regarding version 5010, go to edocket.access.gpo.gov/2008/pdf/E8-19296.pdf. ■