Healthcare RISK MANAGEMENT

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

October 2013 | Vol. 35, No. 10 Pages 109-120

Salespeople in operating room pose risks, require vetting and guidelines

Vendor credentialing by outside companies gaining more attention

As much as risk managers might like to tightly control access to patient care areas and other sensitive parts of a healthcare facility, the nature of the business requires having salespeople and other vendors on-site regularly. Perhaps the most invasive visitor is the salesperson who needs to be in the operating room (OR) during surgery to provide guidance to a doctor using new equipment.

Hospitals are tightening their policies and procedures on those visitors, with many implementing requirements for training in infection control and OR protocol, along with immunizations and background checks. **Dan Flynn**, a surgical instrument sales representative with K&D Medical in Columbus, OH, has been visiting ORs during procedures for 35 years and says hospital policies have changed a great deal in that time.

"They had to put a stop to the free flow of reps going into the OR. It was just too much," Flynn says. "Thirty-five years ago, there were just a handful of us going into the OR, and we were trained, and the hospitals knew they could trust us. Now there are so many reps that hospitals are saying they need some way to certify us and verify that we can be there without threatening patient safety."

> *"Thirty-five years ago, there were just a handful of us going into the OR ... and the hospitals knew they could trust us."*

Hospitals have always expected surgical salespeople to be knowledgeable about OR procedures and never interfere with the procedure, Flynn notes. They are not allowed to make a sales pitch of any kind during the procedure, he says. Rather, they are there to observe, for their own benefit, and to offer guidance to the surgeon on how best to use the instrumentation. Most equipment manufacturers provide training for their salespeople on how to conduct themselves properly in an OR or other patient care setting.

However, now hospitals are requiring more formal training in bloodborne pathogens, privacy issues, and similar concerns, Flynn says.

INSIDE

cover

AHC Media

www.ahcmedia.com

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

Avoid liability with training

The increased focus on vendor credentialing is necessary to protect patients and avoid significant liability risks, says **Sharona Hoffman**, JD, professor of law and bioethics, Edgar A. Hahn professor of jurisprudence, and co-director of the Law-Medicine Center at Case Western Reserve University School of Law in Cleveland, OH.

It is prudent to require training of salespeople before allowing them in the OR, she says. At a minimum, the person must be briefed on protocol and the major do's and don'ts during surgery, she says. It would be better to have a formal training program on all the issues of concern, she says. Also, Hoffman says risk managers should require that the salesperson have a good reason for being in the OR.

"It's reasonable to say that the surgeon is using a new instrument or device and might need some advice from the salesperson during the procedure. That is a legitimate reason to be there," Hoffman says. "If the salesperson wants to be there just to see the device in use, to gather information for the manufacturer, that's probably acceptable too. If the person wants to be there just out of curiosity, probably not."

Require HIPAA compliance

Patient privacy is a significant concern. The vendor does not have a formal relationship with the patient and therefore is not legally required to comply with Health Insurance Portability & Accountability Act (HIPAA), Hoffman notes. However, the hospital should require compliance as part of its approval process, she says. *(See the story on p. 112 for more on patient privacy.)*

"The visitor in the OR should be required to follow all privacy rules, and that means they have to understand HIPAA and how it can be violated," Hoffman says. "There are obvious restrictions like no video cameras or photographs, but the salesperson also should be required to follow all HIPAA requirements just as if he or she was an employee of the hospital."

Most hospital systems are using an outside credentialing company to verify that the vendor is safe to allow on-site and in certain situations, such as surgery, Flynn says. The hospitals are

Executive Summary

Hospitals are taking a stricter approach to allowing salespeople in the operating room (OR) during surgery. Other vendors also pose risks if not properly vetted and their actions at the hospital aren't limited.

- ✦ Some hospitals rely on outside credentialing companies to check the visitor's qualifications.
- ✦ More hospitals are requiring situation-specific training for vendors who will be in patient care areas.
- ✦ The potential for liability and negative media attention is high if a vendor contributes to an adverse event.

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 and at additional mailing offices.

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

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

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

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

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

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

SUBSCRIBER INFORMATION

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

Subscription rates: U.S.A., one year (12 issues), $499. Add $17.95 for shipping & handling. Outside U.S., add $30 per year, total prepaid in U.S. funds. For approximately 15 CE nursing contact hours, $545. Discounts are available for group subscriptions, multiple copies, site-licenses or electronic distribution. For pricing information, call Tria Kreutzer at 404-262-5482. Missing issues will be fulfilled by customer service free of charge when contacted within one month of the missing issue date. Back issues, when available, are $87 each. (GST registration number R128870672.)

Editorial Questions

Questions or comments? Call **Greg Freeman,** (770) 998-8455.

turning to these outside companies to do all the verification, which frees them of that administrative burden but still gives them assurance that the vendor has been properly vetted.

To be credentialed by these companies, the salespeople and other vendors often are required to complete courses in specific areas of study, such as infection control. Two of the most prominent companies offering vendor credentialing are Intellicentrics in Flower Mound, TX, which provides the Reptrax vendor credentialing service, and Vendormate in Atlanta. *(See the story below for more on how these services are provided.)*

Relying on those companies can be a practical solution, Hoffman says, because the third party might do a more thorough job of checking the person's background and training him or her than the hospital would. However, she points out that handing the responsibility over to a third party works only if you know that party's stamp of approval is meaningful. To find out, delve into exactly what the company requires and how it trains people.

"When they say training, do they mean a five-minute video or something more substantive?" Hoffman says. "You have to know exactly what it means when they say someone is credentialed."

Companies offer free services

Reptrax and Vendormate services are provided to hospitals at no cost, with the salesperson or the employer paying for the credentialing, explain **Greg Goyne**, vice president of marketing at IntelliCentrics, and **Gary Johnson**, chief marketing officer at Vendormate. About 5,000 facilities in the United States use the Reptrax system, with about 400,000 vendors credentialed. Vendormate has about 1,900 facilities using its system and 63,000 companies credentialed. The companies can credential individuals and companies.

"The hospital has a way of verifying credentials that is more complete and more efficient than trying to collect paperwork from each visitor," Goyne says. "If The Joint Commission audits you, the credentials are available right away."

The credentialing companies can help a hospital achieve the level of scrutiny that most risk managers say they want of vendors, but which can be too much work for the hospital staff, Johnson says. "We see our job as making that process work as easily and effectively as we can for both parties, the healthcare provider and the vendor," Johnson says.

From a salesperson's perspective, the vendor credentialing can be a valuable service, Flynn says. He cautions risk managers, however, not to depend entirely on the word of an outside company when vetting a salesperson or other vendor.

"The credentialing they offer is trustworthy, but remember that they're also in the business of making money by requiring coursework and giving us the blessing that we need to get in the hospital and do our jobs," Flynn says. "The documentation shows that you took the courses, but it doesn't necessarily show that you understand what goes on in the OR and how to conduct yourself. That comes from experience."

SOURCES

- **Dan Flynn**, Sales Representative, K&D Medical, Columbus, OH. Email: dflynn64@gmail.com.
- **Greg Goyne**, Vice President of Marketing, IntelliCentrics, Flower Mound, TX. Telephone: (972) 316-6523. Email: ggoyne@intellicentrics.com.
- **Sharona Hoffman**, JD, Professor of Law & Bioethics; Edgar A. Hahn Professor of Jurisprudence, Co-Director, Law-Medicine Center, Case Western Reserve University School of Law, Cleveland, OH. Telephone: (216) 368-3860. Email: sxh90@case.edu.
- **Gary Johnson**, Chief Marketing Officer, Vendormate, Atlanta. Telephone: (404) 949-3402. Email: gary.johnson@vendormate.com. ✦

Companies offer vendor credentialing for hospitals

Relying on an outside company to credential vendors can result in more thorough vetting of hospital visitors and help you avoid a significant administrative burden, according to representatives from the two most prominent companies providing the service.

Hospitals that designate Reptrax as their credentialing service can determine what qualifications they require for salespeople or other vendors, and then the service will take responsibility for verifying that those standards are met, says **Greg Goyne**, vice president of marketing at IntelliCentrics in Flower Mound, TX, which provides the Reptrax vendor credentialing service.

Reptrax and Vendormate keep on file all the records showing the person's credentials. Those records might include training courses completed, immunizations, criminal background checks, and whether the person is on any healthcare-related watch lists for exclusion related to fraud. Both companies check for updates to the exclusion lists every month.

Once the vendor is credentialed by one of the companies, that information is available to all hospitals that use that company for verification. The vendor only has to provide the credentials once rather than doing it for each hospital visited. Information is updated in real time, but it is posted in the system only after an employee of the verification company has seen the document and confirmed it is legitimate.

When a hospital decides to use one of the companies, it makes credentialing by that company a requirement for access to the facility. Both companies provide kiosks in the hospital where

salespeople and other vendors can check in and print a document showing they are approved by the credentialing company. The kiosks can print identification badges denoting what area of the hospital the person is allowed to visit.

"If the person tries to check in and the credentials do not meet the requirements of this hospital, access will be denied, and an alert will be sent to an administrator," Goyne says.

The hospital can drive the credentialing process, says **Gary Johnson**, chief marketing officer at Vendormate in Atlanta. By declaring that all vendors must be credentialed and have a badge for each visit, the vendors will respond by seeking the proper credentialing from the company specified, he says. The key, however, is that the hospital staff must enforce the hospital's own policies regarding vendors on site.

"If the OR staff says this is a salesperson who's been here every Tuesday for five years and we know him, so it's OK if he doesn't have a badge, everything falls apart. That can be the weak point," Johnson says. "You need to push for 100% compliance for any nonemployee walking your hallways." ✦

Inform patients that sales rep might be in OR

In addition to concerns over patient safety when salespeople are allowed in the OR, risk managers should consider requiring that patients be notified of the person's presence, says **Sharona Hoffman**, JD, professor of law and bioethics, Edgar A. Hahn professor of jurisprudence, and co-director of the Law-Medicine Center at Case Western Reserve University School of Law in Cleveland, OH.

"I think most patients would be pretty surprised to learn that there were people in the OR who were not doctors or nurses," she says. "It would be prudent to include that in the informed consent documents, and that would have to include giving the patient the opportunity to say no, to opt out of having outsiders in the OR during the procedure."

Informing the patient is not required by law, and some would argue that it's not even necessary in terms of ethical concerns. However, Hoffman says hospitals take a significant risk by allowing vendors in the OR without telling the patient. If the salesperson somehow contributed to an adverse event — by compromising a sterile field, for example, or distracting the surgeon — the hospital could be accused of negligence for allowing that person in the room. That liability is especially the case if the hospital could not prove that it adequately vetted the vendor.

Also, a plaintiff's attorney could make much of the revelation that a salesperson was present even if the vendor had nothing to do with the adverse outcome or even if the procedure went well, Hoffman says.

"Patients could just be upset that there are people there who are not directly involved in their medical care," she says. "This is the kind of issue that can lead to lot of ill will, bad publicity, once the patient makes his or her dissatisfaction public. The patient may have no damages and no real lawsuit to pursue, but you could still suffer bad press from allegations that you did not respect the patient's privacy." ✦

$26 million settlement holds lessons for risk managers

A healthcare system's recent settlement with the Department of Justice (DOJ) illustrates a risk posed by consultants who believe they have found fraud, legal experts say. The $26 million settlement involved fraud charges brought by a consultant who said the healthcare system charged inpatient fees for what should have been outpatient treatment.

Shands Teaching Hospital & Clinics, Shands Jacksonville Medical Center, and Shands Jacksonville Healthcare (collectively Shands Healthcare), which operate a network of healthcare providers in Florida, will pay the government and the state of Florida $26 million to settle allegations that six of its healthcare facilities submitted false claims to Medicare, Medicaid, and other federal healthcare programs, the DOJ announced recently.

Allegedly, from 2003 through 2008, six Shands hospitals knowingly submitted inpatient claims to Medicare, Medicaid, and TRICARE for certain services and procedures that Shands Healthcare knew were correctly billable only as outpatient services or procedures, the DOJ reports.

The six Florida hospitals were named as defendants in a *qui tam*, or whistleblower, lawsuit brought under the False Claims Act, which permits private citizens to sue on behalf of the government and receive a portion of the proceeds of any settlement or judgment awarded against a defendant. The lawsuit was filed in federal district court in Jacksonville, FL, by **Terry Myers**, the president of a healthcare consulting firm, YPRO Corp. Of the $26 million settlement, $25,170,400 will go to Medicare and other federal healthcare payers. The settlement also resolved allegations under the Florida False Claims Act; the state of Florida will receive $829,600. Myers' portion

of these recoveries has yet to be determined. *(See the story on p. 114 for Shands' statement on the settlement. See p. 114 for more on the trend toward whistleblower claims regarding inpatient billing.)*

The settlement does not necessarily mean Shands willfully committed fraud, says **Gary C. Matzner**, JD, a partner with the law firm of Kopelowitz Ostrow in Coral Gables, FL. He previously was outside counsel for a large hospital system. "The billing system is incredibly complex, and I think it's more likely that this was aggressive billing but not intentional fraud," Matzner says. "It could be that this was unintentional, but it's always going to be characterized by a whistleblower as fraud."

Noteworthy in this case is the fact that the whistleblower was a consultant, Matzner says. Hospitals should require a confidentiality agreement with consultants that would prevent such charges or at least make them less damaging, Matzner says. "And when I say confidentiality agreement, I mean the long form, not the short form," he says.

The confidentiality agreement would make it difficult for the consultant to find a situation that might sustain a fraud charge and then run with it for personal gain, Matzner says. *(See p. 114 for more tips on how to prevent a consultant from becoming a whistleblower.)*

Gregory Charleston, CPA, CFA, senior managing director with the consulting firm of Conway MacKenzie in Atlanta, sees two possibilities for how a healthcare system can amass $26 million in liability over six years, both equally concerning.

First, he says, healthcare reimbursement is made up of multiple complex rules. If a healthcare organization does not take great measures to hire and train adept staff and to oversee and internally audit reimbursement practices, this kind of exposure can grow quite rapidly. Even in large hospitals there usually are one or two experts in reimbursement, and the hospitals depend on those persons to keep them out of hot water, he notes.

If that person loses focus or leaves the facility, the hospital inadvertently can rack up a significant amount of incorrectly coded claims, he says. "That can carry on for years, and when it's found it's a $26 million problem," Charleston says. "The risk manager has to point to this area and say, `we can't cut corners on staffing and training in this position.'"

Second is the possibility of intentional fraud. "The mounting financial pressure on healthcare organizations can lead to a breakdown of integrity and create situations where professionals look for ways to cut corners and cheat the government," Charleston says. "The board of directors of a health system has a fiduciary duty to make certain that integrity and following the rules are priorities of the leadership of the organization."

> *"The mounting financial pressure on healthcare organizations can lead to a breakdown of integrity ..."*

The DOJ has not imposed a corporate integrity agreement on Shands, notes **Virginia Gibson**, JD, partner with the law firm of Hogan Lovells in Philadelphia. That situation is a strong indication the OIG is satisfied that Shands' current billing systems are compliant and have sufficient checks and balances to make certain these kinds of billing problems do not happen again, she says. "The allegations were that there were no protocols in place for billing, which would be unusual these days," Gibson says. "We don't know if that is true, but if it is, that would certainly be a major failing."

Gibson also wonders why utilization review did not reveal inconsistencies with the care provided and the billing. A possible explanation is that the provider's internal systems did not communicate sufficiently well with each other, with problems detected in utilization review not generating a report to billing or compliance, she says.

"The Shands case is a high dollar version of what we're seeing at a lot of other hospitals," Gibson says. "The rules are not always crystal clear, and we're learning that the government and whistleblowers are looking at admission criteria and billing criteria to see if hospitals are making an effort to follow those rules."

SOURCES

- **Gregory Charleston**, CPA, CFA, Senior Managing Director, Conway MacKenzie, Atlanta. Telephone: (770) 628-0800. Email: gcharleston@conwaymackenzie.com.
- **Virginia Gibson**, JD, Partner, Hogan Lovells, Philadelphia. Telephone: (267) 675-4635. Email: Virginia.gibson@hoganlovells.com.
- **Gary C. Matzner**, JD, Partner, Kopelowitz Ostrow, Coral Gables, FL. Telephone: (305) 384-7644. Email: matzner@kolawyers.com. ✦

Executive Summary

Shands Healthcare in Florida will pay $26 million to settle allegations of false claims. A contractor first accused the provider of defrauding Medicare, Medicaid, and other federal healthcare programs.

✦ The federal Department of Justice claimed that procedures billed as inpatient should have been billed as outpatient.
✦ The case highlights the risk of consultants allowed to work in the health system and to leave it without disclosing concerns about possible fraud.
✦ Risk managers should institute specific policies regarding the responsibilities of consultants who suspect fraud.

Inpatient billing on the feds' radar screen

The $26 million to be paid by Shands Healthcare in Florida is huge, but it is no surprise that a settlement of this size involved inpatient vs. outpatient billing, says **Laura F. Laemmle-Weidenfeld**, JD, partner with the law firm of Patton Boggs in Washington, DC. The federal government has been watching closely for fraud in that area lately, she says.

"It is critical for risk managers to do their best to make sure they are complying with federal government inpatient billing requirements," she says. "It has always been important to do that, but knowing it is directly in the middle of the government's radar screen should provide even more motivation."

Plaintiffs' attorneys also are focusing on inpatient admissions, so Laemmle-Weidenfeld expects to see more whistleblower cases similar to the Shands allegations. Billing mistakes alone are not fraud, she notes, but the hospital must be able to show that it was doing its best to comply with the complex billing rules. To do that, the hospital must hire competent people and have policies and procedures that minimize the risk of error, she says.

"An effective compliance program will help audit and review billing, and even though that will sometimes find problems, it is a lot more effective to find those problems in process and fix them rather than allowing wounds to fester over years and find yourself in an investigation for fraud," Laemmle-Weidenfeld says. "If you identify problems and fix them, the government might still come along and say you were billing wrong for a period of time, but you can show that you weren't being deliberately ignorant or recklessly disregarding. That's the standard of the False Claims Act."

SOURCE

• Laura F. Laemmle-Weidenfeld, JD, Partner, Patton Boggs, Washington, DC. Telephone: (202) 457-6542. Email: llaemmle@pattonboggs.com. ✦

5 steps to avoid multi-million penalties for false claims

To avoid having your consultants and employees turn into whistleblowers, **Gary C. Matzner**, JD, a partner with the law firm of Kopelowitz Ostrow in Coral Gables, FL, advises following these steps:

1. Specify that all work done by the consultant on your behalf is "work product."

This is a legal term that means the information cannot be shared with any third party, unless otherwise required by law.

2. Require that the consultant bring any suspected fraud to your attention immediately.

The contract should include an affirmative duty for the consultant to notify the hospital in addition to and in advance of notifying any third parties of suspected fraud.

3. Use a departure affidavit regarding fraud.

Require that the consultant sign an affidavit at the end of the project declaring no knowledge of fraud or suspected fraud. This document will demonstrate that you sought any information about fraud and that the consultant did not notify you at the time. If the consultant later tries to blow the whistle, an explanation will be needed for why nothing was conveyed to the healthcare provider at the time. The departure affidavit shows you acted in good faith and tried to ferret out any suspected fraud.

4. Require a similar statement from employees.

Annual or semi-annual reviews should include a statement from the employee that he or she has no knowledge of any fraud and understands that the employer requires any suspected fraud to be reported immediately. Also require a similar statement from the employee when terminating employment.

5. Provide a comment line rather than a fraud hotline.

Some health systems provide phone hotlines and encourage employees to report suspected fraud, but that type of hotline often carries a stigma that can deter usage. Instead, provide a phone line on which people can report fraud but also make suggestions and ask questions. Reporting fraud still might be the goal, but the hotline will get more use if the employee does not feel like it is only for snitching on other employees. ✦

Shands cites 'inconsistent billing processes,' makes changes

Shands Healthcare in Gainesville, FL, acknowledges that its hospitals might have billed Medicare and Medicaid improperly but says the overcharges were the result of faults in its billing system and not intentional fraud.

The system recently agreed to pay $26 million to settle fraud claims brought under the False Claims Act by a former consultant. The whistleblower had been hired as an independent con-

sultant by Shands in 2006 and 2007 to conduct a routine audit of its billing practices. The audit showed inconsistent billing processes in 2006 and 2007. Allegedly, for some patients, Shands might have billed Medicare and Medicaid for short overnight inpatient admissions rather than for less expensive outpatient or observation services. In each case of alleged overbillings, the patient received all services ordered.

"We hold ourselves accountable for the highest standards of care and service. The case in question does not involve the failure to provide high-quality patient care, but rather inconsistent billing processes," CEO **Timothy M. Goldfarb**, said in a statement released by the company. "We proactively initiated an independent audit that identified some opportunities to improve billing processes at Shands. We took immediate steps to make improvements."

Shands officials fully cooperated with the state and federal investigation and negotiated the settlement agreement to avoid long and costly litigation, Goldfarb says.

"Shands regularly and proactively conducts audits of its billing practices," the statement says. "It makes constant improvements to remain current with the complicated, evolving health care regulatory environment, which is subject to continued change in policy and guidelines. Shands encourages staff to be active participants in the compliance process and to identify and report potential issues and errors through employee orientation, mandatory annual in-services, year-round communications and promotion of employee compliance hotlines, and other efforts to raise awareness of compliance accountability."

Changes made to Shands' processes and procedures have included:

- improvements to case management protocols and utilization review processes with an improved team approach to accurately assess and code the care provided;
- the use of improved software;
- implementation of new policies and procedures;
- supplemental employee training;
- the engagement of expert physician advisors who help assess coding and are on staff 24/7.

"As a responsible corporate citizen, our intent and practice has always been to comply with government regulations. We have conscientiously worked to create and operate an appropriate, fair and accurate billing system for all payers," Goldfarb says. "There was no intentional misconduct or callous disregard of these issues on our part." ✦

Internal investigations can be best fraud defense

Internal investigations are the best way to detect fraud in your healthcare system and can substantially reduce the fallout from any improprieties found then or later, says **J. Scott Newton**, JD, shareholder with the law firm of Baker Donelson in Jackson, MS.

The $26 million settlement by Shands Healthcare in Gainesville, FL, is a good example of how an internal investigation can mitigate the damages from a spate of improper billing, he says. *(For more on the Shands case, see the story on p. 112.)*

Inpatient billing is likely to remain the hot topic for government investigators for a while, Newton says, so risk managers should conduct internal investigations in that area. Following the $75 million Medtronic settlement in 2008, the government launched what would become a successful, high profile, national initiative targeting hospital inpatient kyphoplasty admissions, which fraudulently increased Medicare reimbursement because the minimally invasive procedures could have safely been performed as an outpatient or observation service.

"While the Shands case involves a different relator and allegations, the similarity of the OIG [Office of Inspector General] investigations clearly indicates that enforcement efforts will remain focused on admission status as a proven way to utilize limited resources to maximize False Claim Act [FCA] recoveries," Newton says. "In addition to the OIG's efforts, physician decisions to admit certain inpatients and subsequent Part A claims by hospitals have been increasingly retroactively denied by Medicare administrative contractors [MAC] and recovery audit contractors [RAC] for failing to be reasonable and necessary."

It doesn't help that the rules are constantly evolving. After hospitals enjoyed success on appeals before administrative law judges, the Centers for Medicare and Medicaid Services (CMS) issued an administrative policy and proposed rule in March 2013. The interim policy allowed hospitals to resubmit Part B claims after a Medicare contractor determined that hospital inpatient services should have been provided on an outpatient basis. On Aug. 2, 2013, CMS published the *2014 Inpatient Prospective Payment System (IPPS) Final Rule*, which is

effective as of Oct. 1, 2013.

The final rule revises CMS criteria for coverage of Part A inpatient hospital claims and adopts CMS' proposal to allow Part B billing of many hospital services following the denial of a Part A inpatient admission based on medical necessity, Newton explains. The final rule benefits hospitals because it increases the number of services hospitals could rebill after a claim is denied for not being reasonable and necessary or when a hospital undertakes a self-audit to determine that the services should have been provided as outpatient, rather than in an inpatient setting.

With the increased enforcement efforts, internal investigations offer the best way to detect and prevent fraud, determine its scope, defend government investigations, ensure compliance, and protect the provider's financial position and public image, Newton says. Hospitals conducting internal investigations must obtain accurate information and respond appropriately while maintaining confidentiality of the investigation and preventing inadvertent disclosure, he advises.

"Employee interviews, document reviews, the preparation of the defense, controlling the flow of information, including document retention, and investigative reports all potentially present difficult attorney-client privilege and work product problems," he says.

Executive Summary

Internal investigations offer the best way to detect and prevent fraud, determine its scope, and defend government investigations. Learning the scope of the problem as early as possible affords the best opportunity to prevent or limit damages.

- ✦ Inpatient admissions are particularly challenging for compliance.
- ✦ CMS rules on billing change frequently, and policies must be updated.
- ✦ An internal investigation can help avoid criminal charges.

For this type of fraud to be prevented, senior management has to know that their compliance programs are effective and where they are not, and make necessary changes to ensure meaningful implementation, Newton says. "One thing that strikes me about the CMS changes is they could have a practical impact on fraud cases by providing defense counsel a better argument with federal prosecutors and the OIG for an offset before single damages are determined as part of a FCA [False Claims Act] settlement or at trial," he says.

Learning the scope of the problem a provider faces as early as possible affords the best opportunity to prevent criminal, civil, or parallel actions and limit damages, particularly if the government has not begun an investigation, Newton says. Preventive action might be taken early to eliminate the intent or knowledge necessary for the government to prosecute a case or to significantly limit exposure.

When the investigation has begun, obtaining a declination of the criminal case against the provider and its senior management is obviously the priority. In some cases, cooperation can be an effective way to obtain the declination and begin defending the civil case, Newton says.

"The importance of relationships and knowing the needs of individual investigators and prosecutors, including their case loads, is also critical," he says. "Moreover, knowing creative ways to reduce time periods for the alleged fraud or penalties, thereby reducing the aggregate settlement, as well as having experience arguing things like the passage of the statute of limitations, inability to pay, or public policy issues can further limit exposure."

SOURCE

• J. Scott Newton, JD, Shareholder, Baker Donelson, Jackson, MS. Telephone: (601) 351-8914. Email: snewton@bakerdonelson.com. ✦

Photocopiers seen as HIPAA risk after $1.2 million payout

Of all things, now you have to worry about photocopiers. A health plan recently agreed to pay $1.2 million for breaching the Health Insurance Portability & Accountability Act (HIPAA) by leaving protected health information (PHI) on the hard disk of a photocopier it sent back after leasing it. The Department of Health and Human Services (HHS) is warning providers that such breaches are more likely than you might have imagined.

Affinity Health Plan will settle potential violations of HIPAA for $1.2 million, HHS reported recently. Affinity Health Plan is a not-for-profit managed care plan serving the New York metropolitan area. *(See the story on p. 118 for more details on how the breach was detected.)*

Office of Civil Rights (OCR) Director **Leon Rodriguez** said in his announcement that the settlement illustrates an important reminder about equipment designed to retain electronic information. "Make sure that all personal information is wiped from hardware before it's recycled, thrown away, or sent back to a leasing agent," he said "HIPAA-covered entities are required to undertake a careful risk analysis to understand the threats and vulnerabilities to individuals' data and have appropriate safeguards in place to protect this information."

In addition to the $1.2 million payment, the settlement includes a corrective action plan requiring Affinity

to use its best efforts to retrieve all hard drives that were contained on photocopiers previously leased by the plan that remain in the possession of the leasing agent and to take certain measures to safeguard all PHI. *(For more information on safeguarding sensitive data stored in the hard drives of digital copiers, go to http://1.usa.gov/15q6Jmf.)*

Executive Summary

The Department of Health and Human Services (HHS) is warning that photocopiers can be the source of significant breaches of private data. A health plan recently agreed to pay $1.2 million to settle claims that it breached privacy rules by leaving protected information on a photocopier.

- ✦ The provider sent a leased photocopier back to the vendor without removing data.
- ✦ Modern photocopiers and other devices have hard drives that can store information.
- ✦ Risk managers should consider whether they have returned leased equipment in the past without wiping data.

Easy to overlook photocopiers

The Affinity settlement is a reminder that PHI can show up in unexpected places, says **Dianne J. Borque**, JD, an attorney with Mintz Levin in Boston. Most people would not immediately think of a photocopier as storing PHI because we think of the machines as merely copying an original, Borque notes. But today's photocopiers aren't like those of a generation ago that needed you to remember only to take your original off the glass before leaving.

"Computers and laptops are not the only devices with hard drives," Borque says. "Photocopiers, fax machines, notebooks and PDAs [personal digital assistants] are all devices with internal storage drives where PHI can reside and must be protected."

She notes that the fine might not even be the worst result for Affinity. "Large fines are bad, but corrective action plans can also be harsh — and expensive," Borque says. "Affinity's corrective action plan requires comprehensive follow-up on a tight timeframe and with strict oversight by OCR. Affinity is responsible for its own expenses in implementation."

Part of Affinity's corrective action plan is track down all the other hard drives they forgot to wipe. Borque notes that, hearing of this settlement, a lot of other hospitals might be doing the same backtracking. *(See the story on p. 118 for more on what do about that problem.)* "This settlement is a teachable moment. You can send a reminder that someone got in a heap of trouble because they forgot to wipe the data on a photocopier," Borque says. "You'll get a lot of people saying they never even thought of that risk."

The OCR sent a clear message to the healthcare industry, says **Joseph S. Abrenio**, JD, partner with the law firm of LeClairRyan in Alexandria, VA. Abrenio notes that the Federal Trade Commission (FTC), along with the National Institute of Standards and Technology, offers covered entities advice and guidance on how to properly secure and destroy electronic PHI from photocopier hard drives. "Most importantly, photocopiers should be maintained and monitored by appropriately trained IT staff," Abrenio says. "Secondly, data protection technology, such as encryption and data overwriting software, should be used to ensure the security and, when necessary, the destruction of PHI. Finally, a covered entity should have written policies and procedures related to the use and disposal of photocopiers."

> *"Make sure that all personal information is wiped from hardware before it's recycled, thrown away, or sent back to a leasing agent."*

Technological safeguards are covered largely by the security rule, one part of HIPAA that can go overlooked and lead to breaches such as this one, attorneys say. The security rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic PHI. *(See the story on p. 118 for more information on the security rule.)*

The settlement should prompt risk managers to pay a visit to their security officer and discuss the serious ramifications of such an oversight, says **James A. Hoover**, JD, partner with the law firm of Burr & Forman in Birmingham, AL.

"Ask what your organization has done in this area. Do you have procedures in place to scrub these hard drives before you return equipment to the leasing company? Do you have an inventory of the hard drives that could contain PHI?" he asks. "If you don't have those policies and procedures, you need to develop them pretty quickly."

SOURCES

- **Joseph S. Abrenio**, JD, Partner, LeClairRyan, Alexandria, VA. Telephone: (703) 647-5936. Email: joseph.abrenio@leclairryan.com.
- **Dianne J. Borque**, JD, Member, Mintz Levin, Boston. Telephone: (617) 348-1614. Email: dbourque@mintz.com.
- **James A. Hoover**, JD, Partner, Burr & Forman, Birmingham, AL. Telephone: (205) 458-5111. Email: jhoover@burr.com. ✦

Affinity reported its breach after media tip

Officials at Affinity Health in New York had no idea they had lost protected health information (PHI) until they were notified by a news outlet. But then they reported the breach to federal investigators.

Affinity Health Plan will settle potential violations of the Health Insurance Portability & Accountability Act (HIPAA) for $1.2 million. Affinity filed a breach report with the Health and Human Services Office for Civil Rights (OCR) on April 15, 2010, as required by the Health Information Technology for Economic and Clinical Health (HITECH) Act. The HITECH Breach Notification Rule requires HIPAA-covered entities to notify HHS of a breach of unsecured PHI.

Affinity indicated that it was informed by a representative of CBS Evening News that, as part of an investigatory report, CBS had purchased a photocopier previously leased by Affinity. CBS informed Affinity that the copier that Affinity had used contained confidential medical information on the hard drive.

The health provider estimated that up to 344,579 individuals might have been affected by this breach. OCR's investigation indicated that Affinity impermissibly disclosed the PHI of these affected individuals when it returned multiple photocopiers to leasing agents without erasing the data contained on the copier hard drives.

In addition, the investigation revealed that Affinity failed to incorporate the electronic PHI stored on photocopier hard drives in its analysis of risks and vulnerabilities as required by the Security Rule, and it failed to implement policies and procedures when returning the photocopiers to its leasing agents. ✦

OMG! How many of our hard drives are out there?

The news of Affinity Health Plan in New York paying a big fine for sending a leased photocopier back without wiping the protected health information (PHI) from its hard drive may have risk managers wondering if their facility has done the same thing. How many hard drives on photocopiers or other equipment did you let loose in past years with sensitive data?

Leased or sold equipment is not the only problem, notes **Dianne J. Borque**, JD, an attorney with Mintz Levin in Boston. If you are part of a large entity such as a university that has portions covered by the Health Insurance Portability & Accountability Act (HIPAA) and some not, simply moving a photocopier or a fax machine to another office down the hall could be a breach if you don't wipe PHI.

If you are unsure about the status of hard drives that have been sent outside your facility, you already have a problem, Borque says.

"At that point you would have a suspected security incident, and you would need to follow up on that like any security incident at your organization. You have to do due diligence and try to track them down," she says. "If the machines were leased, you have to go to the vendor, and to the new user of that equipment, and hope everyone cooperates with you. If there was a breach, you'll have to decide about disclosing. If you can't find them, you need to document that you made a genuine effort." ✦

Security rule can get short shrift

So much compliance is involved with the Health Insurance Portability & Accountability Act (HIPAA) that it is no surprise some facets get less attention than others. Unfortunately, the security rule is sometimes the part that doesn't get enough attention, says **Matthew L. Kinley**, JD, partner with the law firm of Tredway Lumsdaine & Doyle in Los Angeles.

The settlement by Affinity Health in New York shows the risk of that oversight, he says.

"The security rule says it's not just a matter of having secure systems from IT. It's a process of going through and evaluating where PHI may be lost," Kinley says. "I get the feeling that the fine for Affinity might have been a lot less if they had actually sat down and thought about where PHI might be. It's really just a matter of brainstorming where you might have PHI and then what you should do to keep it from getting out in the world."

Keeping the PHI from escaping might be an IT issue, Kinley says, but identifying all the potential sources of PHI is not. "If they had done that and still hadn't realized that photocopier was out there with PHI, they could have shown that they made the effort, that they were trying to comply with the rule," Kinley says. "I think that could have made a difference in how OCR [Office of Civil Rights] reacted."

The case is a reminder to take an inventory of all the places PHI might reside in your organization, says **Melissa K. Bianchi**, JD, partner with the law firm of Hogan Lovells in Washington, DC.

"It's the first step in a risk assessment, but it's easy to focus on the obvious answers and then move on to the next

step," Bianchi says. "Everyone is going to say laptops and desktop computers, and maybe phones, but the possibilities are so much broader than that. It would help to involve someone in the process who is very tech savvy and can bring up devices that you never imagined might capture PHI in their daily use."

SOURCES

• **Melissa K. Bianchi**, JD, Partner, Hogan Lovells, Washington, DC. Telephone: (202) 637-3653. Email: Melissa.bianchi@hoganlovells.com.

• **Matthew L. Kinley**, JD, Partner, Tredway Lumsdaine & Doyle, Los Angeles. Telephone: (877) 923-0971. ✦

OIG opinion supports remote monitoring

The Office of Inspector General (OIG) of the Department of Health and Human Services (HHS) has issued an advisory opinion that supports an arrangement under which a vendor of technology platforms proposed to contract with hospitals to provide services to patients following hospital discharge.

The OIG concluded that it would not impose penalties under the Anti-Kickback Statute even though the arrangement potentially could generate prohibited remuneration. The OIG further concluded the arrangement would not constitute grounds for the imposition of civil monetary penalties under a provision prohibiting inducements to beneficiaries.

The vendor, a wholly owned subsidiary of a pharmaceutical manufacturer, has developed technology platforms and services that are designed to help hospitals avoid payment reductions associated with excess readmissions by coordinating care and facilitating patient adherence to discharge plans. Fees for the arrangement will include an initial flat fee; an annual fee, based on patient volume, which can be adjusted and increased only if the actual use exceeds the baseline use already paid for by the annual fee; and additional fees for additional services requested by a hospital.

Services provided by the arrangement include the availability of patient liaisons to monitor a participating patient's adherence to the hospital discharge plan and his or her current health status. The services also would include scheduling follow-up appointments, the provision of refill reminders, transportation support, and the generation of reports to help the hospitals monitor the use of the services and readmission rates. The vendor certified that neither the vendor nor nurses contracted by the vendor would promote the pharmaceutical manufacturer's products. In addition, regardless of the patient's question or symptom, the nurses contracted by the vendor would not refer the patient to any provider or supplier other than the patient's established providers and suppliers.

The OIG concluded the arrangement posed a low risk of fraud and abuse under the Anti-Kickback Statute because it is unlikely to lead to increased costs or overutilization. The arrangement also is unlikely to interfere with clinical decision-making, OIG concluded. The services would be rendered after a participating patient is diagnosed and discharged from the hospital.

The OIG also concluded that the arrangement is unlikely to result in inappropriate patient steering. Individuals contracted by the vendor to interact with participating patients would be prohibited from referring the patients to any provider, practitioner, or supplier other than a patient's established provider, practitioner, or supplier.

The full advisory opinion is available online at http://tinyurl.com/oigremote. ✦

COMING IN FUTURE MONTHS

- ✦ Credentialing business associates
- ✦ Disclosure is good for Stark violators
- ✦ Involving everyone in security
- ✦ Should you have drug tests after adverse events?

CNE OBJECTIVES

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

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

CNE INSTRUCTIONS

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

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

CNE QUESTIONS

1. **According to Sharona Hoffman, JD, professor of Law & Bioethics, Edgar A. Hahn professor of jurisprudence, and co-director of the Law-Medicine Center at Case Western Reserve University School of Law, what should hospitals require of salespeople in the OR regarding the Health Insurance Portability & Accountability Act (HIPAA)?**
   A. They are not covered by HIPAA and should not be required to comply.
   B. They are not covered by HIPAA but still should be required to comply.
   C. They are covered by HIPAA, but the hospital is not responsible for their compliance.
   D. They are covered by HIPAA, and the hospital will be held accountable for their compliance.

2. **In the $26 million settlement involving Shands Healthcare, what was at issue?**
   A. Inpatient vs. outpatient billing
   B. Readmissions
   C. Home care supplies
   D. Billing for procedures not performed.

3. **Which of the following is advised by Gary C. Matzner, JD, a partner with the law firm of Kopelowitz Ostrow, to prevent fraud claims by whistleblowers?**
   A. Require new hires or consultants to sign a statement agreeing not to contact third parties regarding suspected fraud
   B. Require departing employees or consultants to sign a statement saying they know of no suspected fraud.
   C. Explain the limitations of the False Claims Act to all employees and consultants.
   D. Designate an individual to receive fraud reports and then forward them on to authorities.

4. **What was one part of the corrective action plan that Affinity Health must undertake following its settlement for a privacy breach?**
   A. Track down photocopiers and other devices with hard drives that might not have been wiped before they were returned to leasing companies.
   B. Institute a monthly wipe of all devices containing protected health information (PHI).
   C. Restrict the number of photocopiers on which PHI can be stored.
   D. Use only photocopiers that do not include hard drives.

Legal Review & Commentary

A Monthly Supplement to HEALTHCARE RISK MANAGEMENT

81-year-old woman's fall from bed after surgery results in $3.5 million verdict

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

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

News: An 81-year-old woman recovering from hip replacement surgery suffered significant injuries including a femur fracture, head injury, and cerebral stroke when she fell from a hospital bed and required an emergent second hip repair surgery. The plaintiff contended that the hospital and its nurse employee were negligent because they had failed to provide reasonable and prudent care. Defendants denied liability and the significance of the damages. The jury assessed $3.5 million in damages against the hospital.

Background: In this matter, the plaintiff was an elderly woman who initially presented to the hospital for a right hip arthroplasty that occurred without incident. Subsequent to the surgery, the patient was a high, if not extreme, fall risk who required fall-prevention interventions. In particular, it was alleged that subsequent to the surgery, she was noted to have advanced age, gait and vision problems, mind-altering medications, and an altered mental status (anxiety, confusion, and tearfulness). The patient was said to be noncompliant with instructions. She repeatedly tried to get out of bed despite instructions to remain in bed, and she tried to remove IV lines, the plaintiff said. It was further alleged that this information was not communicated properly to incoming staff during change-of-shift report. In fact, during the morning shift immediately before her fall, the plaintiff was not assessed for fall risk, and the fall risk assessment record on her chart was left blank, the plaintiff said. These circumstances resulted in the patient falling out of bed, according to the plaintiff. The patient said that her fall caused a femur fracture that required immediate surgical repair, as well as a serious head injury that, within hours of the fall, resulted in a disabling stroke.

... the plaintiff was not assessed for fall risk, and the fall risk assessment record on her chart was left blank ...

She contended that the hospital and the nurse were negligent and had breached appropriate standards of care toward her by, among other things, failing to properly assess her high or extreme fall risk, by failing to monitor her on a timely and meaningful basis, and by failing to employ fall risk interventions such as bed side rails, bed alarms, a sitter, or soft restraints.

The plaintiff demanded $10 million in compensatory damages, and she also demanded punitive damages. Defendants denied liability for negligence, and they also denied the cause of the damages in light of the plaintiff's advanced age and other comorbidities. Members of the jury awarded a verdict of $3.5 million against the hospital, and it subsequently was reduced to $1.8 million under applicable Virginia law capping medical malpractice damages. The jury returned a verdict in favor of the individual nurse.

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

What this means to you: There are an estimated 700,000 patient falls happening in hospitals annually, and roughly one-quarter of those result in injury. Prevention of falls has been and remains a priority for hospitals and other healthcare providers. Indeed, estimates are that between 2-10% of all hospital inpatients fall, and 10% of those suffer serious or severe injuries. Note also that since 2008, the Centers for Medicare and Medicaid Services (CMS) has refused to reimburse hospitals for treatments of complications arising from a fall that results in a fracture or other serious injury. All of that noted, cutting the number of annual falls to zero is probably unrealistic, especially given that sometimes hospitalized patients need treatments that require the risk of mobilization to prevent bed-rest complications such as pressure ulcers and deep-vein thrombosis, or to facilitate physical therapy where weight bearing within a certain amount of time after surgery is recommended.

Falls typically involve elderly patients, and advanced age on its own is a universally recognized risk factor along with confusion, intermittent or recent fall history, and current attempts to get out of bed unassisted. That said, while for those reasons the focus of fall prevention is often on the frail elderly, hospitals must also keep in mind that younger, independent patients often fall as well. These patients are frequently not assessed as being at risk to fall because they are alert, oriented, and capable of independent ambulation. In these cases, younger patients who undergo surgery or other procedures might not realize that they are limited by pain medications, weakness in a limb, disorientation to their environment, or other factors. Their drive to remain independent and their reluctance to call for assistance can make it extremely difficult to protect them from a fall. They often refuse bed alarms, side rails, and restraints. These sorts of patients often need "tough love," and it's important to impress this information upon their family and frequent visitors as well.

When a patient fall occurs in a hospital, the dominant legal theory at issue is almost certainly going to be negligence. Stripped of the legal mumbo-jumbo, what the judge and jury will be looking to determine is whether the hospital and its employees behaved reasonably in light of generally applicable standards of care and the particular circumstances surrounding the particular patient. This examination will give rise to more specific questions such as whether the data concerning the patient was reasonably shared among providers and staff and reasonably interpreted, and whether reasonable steps were taken to prevent the patient from falling.

Every hospital should have a well-established and publicized set of protocols for fall prevention. All providers and staff that interact with patients in any capacity that could relate to a fall incident should be trained concerning these protocols on a periodic and documented basis. Such protocols should include, but not necessarily be limited to, the following:

1. Make sure the patient is familiar with the environment, which even at night should be sufficiently lit by a nightlight or with supplemental lighting to allow the patient the ability to see the call light and controls to increase the amount of light in the room.

2. Make sure the patient at risk can be easily identified by other staff members passing by their room or receiving them in their departments, such as radiology staff. For this purpose, hospitals often use mechanisms such as a colored armband, a sign on the door and on the chart, a brightly colored blanket, gown, or booties.

3. Place signs in the patient's room and the surrounding hallways reminding the patient (as well as visitors) of the possibility and dangers of falls. The signs should remind them to request assistance before getting out of bed.

4. Maintain the call light within easy reach and have the patient demonstrate call light use.

5. Keep personal items within easy reach of the patient on a non-skid surface so they are unlikely to fall off and entice the patient to try to retrieve them from the floor.

6. Place (and maintain) sturdy, secure side rails on patient beds, and handrails in all bathrooms and hallways.

7. Beds equipped with siderails running both sides of the entire length of the bed should be avoided. A patient who climbs over a siderail will fall further and sustain greater injury than a patient who attempts to gets out of the bed between an upper and lower siderail on one side of the bed or the other.

8. Fall mats below the bed are popular and proving to prevent serious injury if a patient should fall.

9. When patients are resting, hospital beds should be in a low position. When the patient needs to get out of the bed to use the bathroom or for therapeutic purposes, the bed should be adjusted to a comfortable height, and the patient should be safely assisted in getting out of the bed.

10. Bed brakes should always be in the locked position, as should wheelchair brakes, unless and until the patient is secured in the bed or wheelchair for transit.

11. The patient should be fitted with footwear that is non-skid and comfortable without being loose.

12. Patient areas should be maintained with a minimum of clutter, and instruments, IV lines, and other cords should be organized to avoid entanglement.

13. Floor surfaces in patient rooms and surrounding hallways should be kept clean and dry; in particular,

any spills should be immediately wiped up, and the spill area should be cleaned and dried right away.

14. Keep high fall risk patients — whether that risk is due to their delicate physical condition, cognitive impairment, or some combination — in a safety zone area as close as possible to the nurses' station and subject to frequent rounding.

15. Bed alarms, individual sitters, and soft restraints are extra interventions that should be seriously considered for high and extreme fall risks.

16. Physical therapists should employ a walker and a gait belt absent compelling reasons to do otherwise in light of the patient's rehabilitation progress.

Also, if a fall occurs, it is important to promptly and accurately document the resulting injuries and steps taken for treatment, and to consult with legal counsel if there are any questions about what should or should not be documented. In the case discussed above, there was also a thread of allegations of improper documentation concerning the head injuries the plaintiff sustained as a result of her fall. The patient said that when she fell, she hit her head on the metal base of her portable tray table. She alleged that the nurse and the hospital kept that information out of the patient's medical record and instead noted that fact in a document they believed the patient might not have been able to access.

There are doctrines such as the attorney-client privilege and the peer review privilege that might apply to shield certain documentation from discovery. However, it is critical that those doctrines are properly applied and not abused or misinterpreted and thus make it appear that the hospital or provider has been trying to cover up information. This appearance of cover-up potentially can lead to several bad developments such as the imposition of discovery sanctions, adverse jury instructions (telling the jury to consider that the hospital tried to hide or destroy information), or even substantively unfavorable rulings on the merits of the case.

Keep in mind that when a patient falls and suffers a head injury, he or she might not remember the fall or the circumstances leading up to the fall. Credible documentation that is as "real-time" as possible concerning the circumstances before, during, and after the incident will be the hospital's best opportunity to demonstrate that it behaved reasonably and that it did not subsequently try to paper the file with documentation shaded in its favor, once it learned that the patient was unlikely to have an independent recollection of the events.

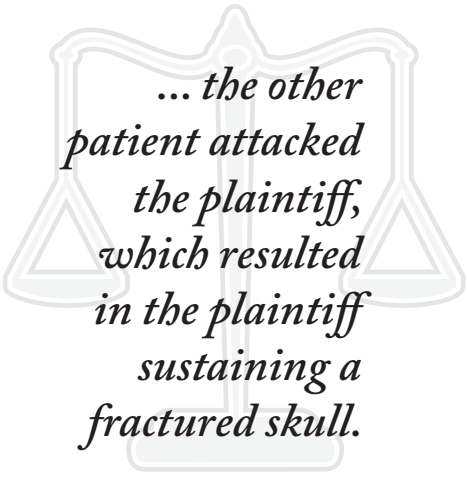
Reference:

Circuit Court of Virginia Case No. CL 1101633F-15 ✦

Negligent placement of patient in room with psychotic patient leads to $6 million verdict

News: The plaintiff, an adult (but non-elderly) male, initially sought treatment at an acute care medical center for his mental health issues. Upon transfer to the defendant behavioral health hospital, plaintiff was put into a room with another patient, who suffered from psychiatric problems that caused him to act violently. The plaintiff said that upon being placed in the room with the other patient, the other patient promptly attacked him and struck him in the head, resulting in the plaintiff sustaining a fractured skull. At trial, the plaintiff was awarded about $6 million in damages.

Background: In this matter the plaintiff was a teacher and private tutor, and he presented at an acute care medical center complaining of suicidal thoughts and depression.



The medical center transferred the plaintiff to the defendant behavioral health facility, which is a private, fully accredited, full-service acute psychiatric hospital that offers behavioral health, substance abuse, and eating disorder treatment options for the local communities. Once admitted to the behavioral health facility, the plaintiff was put into a room with another patient, who is said to have been suffering from acute psychosis causing him to engage in violent behavior, such as a self-inflicted stab wound to the chest. Almost immediately the other patient attacked the plaintiff, which resulted in the plaintiff sustaining a fractured skull.

Discovery in the case revealed that the other patient reportedly had been diagnosed as a paranoid schizophrenic who had been off his medications for several months. When admitted, the other patient had demonstrated erratic behaviors such as ripping out his IV

and attempting to escape, according to records. The plaintiff further claimed that he was placed into the same room as the other patient based upon an error in judgment made by the facility charge nurse. During the admission assessment process, the nurse overlooked the other patient's medical records and assessed him as low risk based on his statements during an interview in which he was sedated, the plaintiff contended.

The plaintiff alleged that his encounter with the other patient resulted in the plaintiff sustaining numerous skull fractures and permanent brain injury, as well as jaw fractures and hearing loss. He remained comatose and on life support for several days, and he had to spend a month in the intensive care unit. The plaintiff said that he now suffers from extreme mood and personality issues and cognitive function deficits that resulted in losing his jobs as a teacher and a tutor, due to inappropriate and unprofessional behaviors that he said he cannot control.

The plaintiff claimed medical negligence, dependant adult abuse, violation of patient's rights, and willful misconduct. The defendant facility denied that it was liable, and said that it did not know of the other patient's propensity of violence toward other people. After a seven-day jury trial, the plaintiff was awarded about $6 million in damages. Court records also indicate that his number was reduced to $2.3 million pursuant to a "high-low" agreement to which the parties had stipulated in advance, although the plaintiff also recovered about $334,000 in attorney's fees and about $118,000 in court costs.

What this means to you: Stripped of the legalese, the primary issue for the hospital was to what degree, if any, it was negligent because it behaved unreasonably in pairing the plaintiff with a patient who had a demonstrated history of mental problems and thus likely posed significant dangers to himself and others. Highlighting the problem here for the defense is that the behavioral health facility provides primarily psychiatric care, and staff members certainly should have known better than to pair someone like the plaintiff with someone like the other patient.

Nonetheless, the case still serves as a good object lesson reinforcing the need to constantly drill physicians and staff of all levels on the importance of not only completing medical charts promptly and accurately, but also taking the time to read and understand patient charts available when performing a patient evaluation or otherwise treating a patient. Patient assessment, whether on admission or at the start of a shift, begins with the medical record. Not knowing a patient's history, including what other providers have documented about the patient in the remote as well as recent past, places the caregiver at risk of missing critical information essential to patient care.

Moreover, today most patients needing psychiatric care present themselves (as the plaintiff here apparently did) or are brought by family or rescue ambulance to acute care facilities that don't have behavioral health units. Finding accepting psychiatric facilities for these patients can be difficult, as the few facilities that remain open often will accept only insured patients who don't have any medical care issues. Housing these patients in emergency departments or in acute care beds until a facility can be found is challenging and extremely high risk. Where do they safely place a violent patient? How are visitors, physicians, staff, and other patients to be kept out of harm's way? To these ends, some hospital emergency departments have established a "safe area" where these patients can be closely observed by staff members and hospital security officers trained in dealing with psychiatric and assaultive behaviors. These seem to be constructive steps in the right direction.

Note also that this case illustrates the successful use of a stipulated "high-low" agreement, in which the parties had agreed before trial that defendant's liability would be capped at a certain number should the jury's verdict exceed that number, while plaintiff's ability to secure a certain amount of recovery would be guaranteed even if the jury were to return a defense verdict or award only minimal damages on a plaintiff's verdict. High-low agreements are commonly employed in arbitrations and other alternative dispute resolution contexts. Although it would be critical to check with counsel before employing a high-low agreement in any particular case, high-low agreements often are viewed with approval by courts. At least one state court system (California) has a statutory scheme dedicated to employing high-low agreements. (See Cal. Civ. Proc. Code Sections 630.01 et seq.) High-low agreements generally are worth considering for hospitals and providers when it appears unlikely, although not impossible, that the hospital or provider will escape liability completely and the goal is to contain damages. The plaintiff and especially the plaintiff's counsel, if operating on a contingency fee, might be willing to trade the shot at a runaway jury verdict for certainty that there will be at least some recovery. Finally, parties contemplating a high-low agreement might also consider a derivative dispute resolution structure called "pendulum" arbitration. It also is known as "baseball" arbitration, in light of its use in salary disputes for professional baseball players. The parties present their respective cases and then submit competing resolution proposals, of which the arbitrator must pick one.

Reference:

Los Angeles County Superior Court Case No. SC110387 ✦