



Healthcare Risk Management™

June 2010: Vol. 32, No. 6
Pages 61-72

IN THIS ISSUE

- Large pill theft shows challenge of securing hospital drugs cover
- Hospital letter details response to thefts 63
- Response plan needed for missing patients 63
- Many patients at risk for wandering, elopement . . . 66
- Criminal background checks a must for providers. 66
- Tips for improving your background checks 68
- HIEs come with privacy and security risks 68
- Start early when obtaining consent for HIE 70
- UCLA worker gets prison for HIPAA violation. 71

Financial Disclosure: Author Greg Freeman, Managing Editor Karen Young, Executive Editor Russ Underwood, 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.

Large pill theft shows challenge of securing hospital drugs

Staff steal 370,000 pills, loss not detected for months

Drug theft is a vexing problem for any health care provider, but a health system in Texas is finding that the thefts can be on such a scale that federal investigators become interested and the community starts asking how the provider could have let the thieves continue for so long.

The Texas State Board of Pharmacy reacted forcefully to the thefts of 370,000 pills from The Parkland Health and Hospital System of Texas by what hospital officials and police say was a coordinated team of health system employees and criminals who sold the tranquilizers and painkillers on the street. In May, it levied \$20,000 in penalties against Parkland for failing to prevent the massive narcotics theft, among the largest fine ever imposed for pharmacy wrongdoing in Texas, according to a statement released by the board of pharmacy.

The hospital system's troubles may not be over, however. Ron Anderson, MD, Parkland's president and chief executive, issued a statement saying the hospital system is cooperating with the federal Drug Enforcement Agency and Justice Department prosecutors as they investigate the narcotics loss. Parkland discovered the problem in 2007 and it alerted regulators and fired some employees, including a supervising pharmacist who the health system

EXECUTIVE SUMMARY

A Texas hospital system is under investigation for a series of drug thefts within the hospital. Employees and outsiders worked together to steal drugs and sell them on the street.

- The health system has been fined, may face other sanctions.
- Safeguards were in place to discourage theft.
- The provider revamped its drug security program and hired a drug diversion officer.

says alerted subordinates to the Parkland investigation.

The federal Drug Enforcement Administration reports The dismissed head pharmacist was identified by the health system and police records as Ronald Woody. A police affidavit indicates he told investigators “he had warned the pharmacy technicians of the ongoing theft investigation and

that they needed to watch their backs, because they were all suspects,” according to *The Dallas Morning News*.

It is important to note that Parkland self-reported the incident and asked the appropriate agencies to investigate, says **Candace White**, spokeswoman for the hospital. The hospital also sent a detailed letter to the State Board of Pharmacy explaining what hospital officials knew of the thefts and what actions had been taken in response. (For details from that letter, see page 63.)

In the letter, the hospital says that “despite its commitment to improving the health and wellness of a culturally diverse community with a growing indigent population, Parkland was the victim of five employees, some of whom operated as a coordinated criminal ring, who abused their positions of trust within Parkland.”

The hospital confirms that during 2007, five Parkland employees and two outsiders stole 500-count bottles of hydrocodone 10/650 mg, hydrocodone 5/500 mg, diazepam, alprazolam, and lorazepam. The drugs cost the hospital \$13,247.59.

Most troubling are reports that the drug thefts went for nine months to a year before being discovered, says **Julie Malida**, SSA, MAAA, principal for health care fraud at The SAS Institute, a software company with a consulting group that addresses fraud and financial crimes, based in Cary, NC.

“With the appropriate inventory tracking and the appropriate data analytics applied against that inventory management, there should never be a 9-month or 12-month period of loss before missing prescriptions are noticed,” Malida says. “Inventory management should require multiple sign-offs before scripts can be dispensed, even if it is an automated dispensing process. Data analytics can examine prior patterns of dispensing and apply sophisticated modeling, rules, and linkages, to determine what spikes may constitute an outlier. This would enable the hospital and/or pharmacy to stop the bleeding before nine to 12 months of losses occur.”

Such an extensive theft ring should not go unnoticed for months if the provider uses a tracking system that records drug inventory and all drug transactions, scanning on a regular basis for variances, Malida says. The data must be reconciled at the end of the day or the end of the week, and then analytics utilized to look for patterns of common-

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), \$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.)
Photocopying: No part of this newsletter may be reproduced in any form or incorporated into any information retrieval system without the written permission of the copyright owner. For reprint permission, please contact AHC Media, LLC. Address: P.O. Box 740056, Atlanta, GA 30374. Telephone: (800) 688-2421. World Wide Web: www.ahcpub.com.

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.

Director of Marketing: Schandale Kornegay.

Managing Editor: Karen Young (404) 262-5423

(karen.young@ahcmedia.com).

Executive Editor: Russ Underwood (404) 262-5521

(russ.underwood@ahcmedia.com).

Production Editor: Ami Sutaria.

Copyright © 2010 by AHC Media, LLC. Healthcare Risk Management® and HRM Legal Review & Commentary™ are trademarks of AHC Media, LLC. The trademarks Healthcare Risk Management® and HRM Legal Review & Commentary™ are used herein under license. All rights reserved.



AHC Media LLC

Editorial Questions

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

alities among any variances, she says.

“The advanced analytics will look for patterns and outliers that will reveal your problem much sooner than letting a year go by and realizing that 60% of your Valium and 10% of your hydrocodone is missing,” she says. “You would never have to wait an entire year to discover those aberrations.”

Data analytics also would help you spot collusion among employees, such as was reported at Parkland. Malida points out that data analytics software will flag details that may be overlooked by investigators, such as the same people being involved in some or all of the thefts, or a pattern such as every tenth pill being stolen, or the same person signing for all the missing prescriptions.

“The first line of defense is having appropriate tracking and reporting processes in place,” she says. “The second step is that, whether you use advanced analytics or not, someone has to be looking at the data on a regular basis. You can have a great inventory control system and security measures in place, but if you don’t look at the data regularly and often, and deeply enough, you won’t know if those measures are working.”

SOURCES

For more information on preventing drug theft in health care facilities, contact:

- **Candace White**, Media Supervisor, Parkland Hospital, Dallas, TX. Telephone: (214) 590-8054. E-mail: candace.white@parknet.phm.org.
- **Julie Malida**, SSA, MAAA, Principal for Health Care Fraud, The SAS Institute, Cary, NC. Telephone: (312) 819-6800, ext. 8809. E-mail: julie.malida@sas.com. ■

Hospital details drug thefts

The theft ring at Parkland Hospital in Dallas was discovered and self-reported to all appropriate agencies by Parkland’s director of pharmacy services, Vivian Johnson, according to a letter the hospital sent to the State Board of Pharmacy.

In that letter, obtained by *Healthcare Risk Management*, the hospital explains that once Johnson discovered the thefts, Parkland conducted its own investigation and spent about \$1.3 million

in system upgrades, additional security measures, and an independent review by Ernst & Young.

The Parkland Police Department’s investigation at the Parkland Prescription Center led to the arrest and indictment of Sharron Benson, a pharmacy technician, who confessed to the diversions at the prescription center, according to the hospital’s letter. Benson has been indicted and is awaiting trial. The police investigation at the Parkland Community Oriented Primary Care Southeast Pharmacy led to the arrest and indictment of several Parkland pharmacy technicians, a drug dealer, and the husband of one of the technicians, according to the letter.

“These individuals were involved in a conspiracy to steal controlled substances from Southeast and sell them on the street,” the hospital’s letter says.

The pharmacist in charge of the prescription centers was fired for alerting the pharmacy technicians that they were being investigated, the hospital reports. That pharmacist was one of the people arrested.

Parkland tells the State Board of Pharmacy that the losses were not the result of a failure to properly oversee the pharmacies. At the time of the loss, the sites of the theft had cameras, locked controlled substance cabinets, card access for cabinets and entrances, and comprehensive policies and procedures that conformed with federal and state law, the letter says.

“Some criminally intentioned individuals simply decided to steal,” the letter explains.

Parkland emphasizes in the letter that it had discovered the drug theft on its own, conducted an investigation, and terminated five employees. The hospital has already spent more than \$1 million to prevent a recurrence of the drug theft, and it has implemented a significant loss prevention program that included the hiring of a drug diversion officer. ■

Wandering patients need response plan

Resident elopement and wandering can be extremely dangerous for patients and costly to the facility if the patient is injured or dies, but many health care providers do not have a formal plan in place to prevent the problem or respond effectively once staff realize a patient is missing.

Patients who wander and elope should be a top

EXECUTIVE SUMMARY

Patient wandering and elopement creates significant risks to patient safety and exposes the facility to liability claims. Risk managers should create an effective program to prevent wandering and elopement and a response plan when patients are missing.

- Elopement is a sentinel event.
- Alzheimer's patients are at high risk.
- Staff should be ready with a search plan.

priority for risk managers, says **Carolyn Caccese, JD**, attorney, Salenger, Sack, Schwartz & Kimmel, New York City. These incidents frequently lead to lawsuits, and the payouts can be significant if the patient is injured or even dies during the absence, she says. (For details on what patients are at risk and how the incidents can lead to lawsuits, see page 66.)

Caccese notes that wandering and elopement go hand in hand with another major worry for risk managers — falls. Many of the same patients who go missing are the same ones at risk for falls, so the liability risk can be heightened.

“Patients who usually wander often have compromised mental states, so falls are very, very common,” she says. “The injuries can range from bumps and bruises to a fractured hip that requires surgery. A lot of these patients who are compromised just can't recover well from the surgery, so a lot of the patients end up passing away within two years of the fall. That makes wandering a very concerning event.”

Caccese notes that the danger exists even if the patient is unable to leave the premises. Elopement from the facility certainly increases the risk in several ways, but a patient who wanders around the hospital or long-term care facility still can be endangered by falls and other hazards, she says.

Nursing staff responsible

Patients wander for various reasons, says **Maria Rosario Gonzales, RN**, a nurse educator in the Veterans Administration Healthcare System in Los Angeles.

“They may seek escape from a psychiatric unit or hospitalization, want to go home, be confused, and just go for a walk,” Gonzales says. “Whatever the reason, the nursing staffs are accountable for the patient's well-being and safety. In the worst-case scenario, a confused patient may wander off and suffer hypothermia or increased medical complications due to hypothermia and may miss necessary cardiac, anticoagulant, or seizure medications.”

In psychiatric settings, the patient may want to escape to attempt suicide, notes **Sharon Valente, RN, PhD**, an adjunct assistant professor at the University of Southern California, Los Angeles.

“Whatever the reasons for the wandering, the nursing staffs are accountable for the patients, and they grieve when patients leave and worry about the serious life-threatening consequences of failing to prevent the wandering,” she says. “In addition, the . . . economic, legal, and professional consequences of wandering are serious.”

Liability dependent on precautions

A health care provider's liability for injuries or death following wandering or elopement will depend on what precautions were taken to prevent the incident and how the facility responded, Caccese says. The safety measures will be evaluated to determine if they were adequate for that location and what was known about the patient's propensity to wander or elope, she says.

“Unfortunately, there are some patients who, even with all the safety measures, can still wander and something bad happens to them. If you can show that you took all the correct, reasonable steps to prevent this tragedy, and nonetheless it still happened, you may be able to successfully defend yourself,” she says. “But if those safety measures were not documented in the file, these cases often settle. These cases can be indefensible if you have a patient with altered mental status and a history of wandering and the record doesn't show any effort to prevent this person from getting out of bed or their room.”

Most facilities have a policy on preventing wandering and elopement, but Caccese stresses that the patient's record must show the staff complied with that policy.

“Having the policy is necessary, but if you don't document compliance, it can do more harm than good,” she says. “It is a big gift to the plaintiff if the policy exists, but there is no evidence that you complied with your own policy.”

Caccese has worked on cases that deal with patients injuring themselves in both hospitals and long-term care facilities due to improper supervision, and most involved confused patients who leave their bed or room and sustain a fall. Often, the patients have been elderly and on medications that contribute to their confusion, she says. In New York, as in some other states, causes of action alleging in negligence and malpractice can

be brought, in addition to a statutory cause of action created by the Public Health Law.

“If the facility deprives a patient of a right or benefit, or violates a federal or state statute, the patient may utilize this theory of liability beyond just a malpractice case,” she explains. “The Public Health Law sets out a minimum amount of damages recoverable, at least 25% of the daily nursing home rate, and even subjects the facilities to punitive damages. Given the wide range of circumstances where this cause of action can be asserted, it is useful for patients and a serious potential liability concern for providers.”

Caccese recounts one recent case in which she represented a woman who fell while trying to exit her bed and, though she was not injured in that incident, the facility did not take any additional precautions to prevent her from wandering. Two days later the woman left her bed, exited her room, and traveled down the hall unnoticed by staff. When the staff realized she had left her room, they searched and found her on the floor where she had fallen after tripping over some wires hanging off of a gurney. She broke her hip and subsequently sued the hospital.

“We ended up settling the case after depositions, because the hospital could not prove it had taken adequate measures, especially after the first fall,” she says. “Their documentation did not show that they placed the patient at risk for falls or elopement. We were able to prove that they violated their own policy.”

Search grid improves response

Gonzales and Valente studied wandering and elopement in the Los Angeles Veterans Administration facility and found that in a six-month period, 16 patients walked off wards without notification to staff, 13 were missing after privileges were granted, 11 failed to return after being given a pass, nine failed to return after fresh air or smoke breaks, and eight inpatients failed to return after they went for a clinic appointment.¹

Most of the patients were reported missing during the day shift, Valente says. After studying the root-cause analyses for the incidents, Gonzalez and Valente made these two key conclusions:

- The lack of unit- or ward-specific search grids slowed the response and caused the preliminary search to be inefficient and ineffective. Staff should be familiar with a response plan that calls for searching the area in a deliberate, coordinated

effort.

- Communication during the searches was repetitive and chaotic. Staff did not reference the physical layout of the unit when giving directions regarding where to search, which prolonged the preliminary search.

After educating the staff about the missing and wandering patient policy, Gonzalez and Valente designed a mock drill to evaluate the effectiveness of the facility’s policy on missing patients. They announced a facilitywide wandering and missing patient mock drill, which required each unit to use a specific grid to search for the missing patient. The first drill used a generic sample grid to show staff how the tool could be of use, and they found that using the unit-specific search grid helped the staff communicate effectively with each other and organize the search to find the patient and reduce the risk that the patient was harmed. The hospital then directed each unit to develop its own specific grid for use in conducting a preliminary search.

Caccese says such an organized program for finding missing programs could significantly reduce the potential liability for patient injury and liability.

“Preventing the wandering or elopement is the best thing, but it is still going to happen sometimes. Having a response plan that is effective, something that is more coordinated and organized than just telling people to look around, will always be good,” she says. “Beyond that, educating your staff about the proper documentation of your compliance with these policies is the best thing you can do.”

REFERENCE

1. Gonzales MRD, Valente S. The wandering & missing patient: reducing the risk for harm & injury, an evidence-based performance improvement project. 2004: Veterans Administration Healthcare System, Los Angeles.

SOURCES

For more information on wandering and elopement, contact:

- **Carolyn Caccese**, JD, Attorney, Salenger, Sack, Schwartz & Kimmel, New York City. Telephone: (212) 267-1950.
- **Maria Rosario Gonzales**, RN, Nurse Educator, Veterans Administration Healthcare System, Los Angeles. Telephone: (310) 478-3711. E-mail: maria.gonzales@med.va.gov.
- **Sharon Valente**, RN, PhD, Adjunct Assistant Professor, University of Southern California, Los Angeles. Telephone: (310) 478-3711. E-mail: sharon.valente@med.va.gov. ■

Many patients at risk for wandering, elopement

Wandering and elopement exist in all health care facilities, but long-term care facilities are at most risk because of the nature of the residents' conditions. Patients with Alzheimer's disease, dementia, autism, and others who cannot help themselves pose a high risk, no matter the setting.

Ten percent of all lawsuits involving long-term care facilities deal with elopements, according to statistics compiled by EmFinders, a Frisco, TX, company that works with law enforcement agencies and emergency responders across the country, as well as with the national 911 system to develop technology to quickly locate and rescue residents of hospitals and other types of facilities who have wandered and become lost. EmFinders is one of many products available to health care providers that can help providers prevent wandering and elopement, or to find patients after they leave.

EmFinders Founder and CEO **Jim Nalley** provides these other facts compiled by his company:

- Elopement is ranked number 11 on The Joint Commission list of Sentinel Events.
- Forty-five percent of elopements occur in the first 48 hours of admission to a facility.
- Elopements reflect the highest severity allegation involving the long-term care setting.
- CNA, the commercial insurance carrier based in Chicago, reports that elopement allegations have had an average total per claim of \$393,650.
- Seventy percent of these lawsuits involve the death of a resident.
- Sixty percent of people with Alzheimer's disease will wander throughout the course of their disability, according to the Alzheimer's Association in Chicago. ■

Background checks protect patients

Background checks for criminal records or other questionable behavior should be a standard risk management strategy for all health care providers, and meeting minimum requirements is not the best way to go, say providers and experts in background screens.

EXECUTIVE SUMMARY

Background checks are an important tool for preventing criminal activity and harm to patients or other employees. Providers should screen thoroughly and understand the common mistakes.

- Not all states require background checks, but providers should do them anyway.
- Do not restrict your search to just your own state's criminal records.
- Approach all information provided by an applicant with skepticism.

About 25% of states require some sort of background screening for health care workers, says **Jenifer DeLoach**, senior vice president with Kroll, a risk consulting firm in Nashville, TN. Even without a state requirement, hospitals and other providers should conduct background checks to protect themselves from claims of negligence if an employee commits a crime, such as assaulting a patient or fellow employee, and turns out to have a criminal history, she says.

"Health care workers have access to vulnerable patient populations, controlled substances, people's private property," DeLoach says. "They also have access to huge amounts of data, including personal financial information. People seeking access to this data, or drugs, or patients they can victimize, will apply and seek positions in hospitals."

DeLoach says risk managers should be especially vigilant now that the economy is down and more people are seeking new career opportunities.

"A lot of folks are very cognizant that nursing is one field that is hiring, so a lot of people are entering nursing programs to start anew," she says. "There's going to be an influx of new talent, and that will mean people who are moving from one state to another for a hiring opportunity. And there can be people in that group who lost their jobs for questionable reasons or who are trying to start over again after a conviction."

Even in states that require a minimum level of screening, providers should consider going beyond that minimum to ensure that the screening is effective, DeLoach says. Budget considerations may limit how much screening can be done, but she reminds risk managers to consider the potential liability from negligently hiring someone with a questionable background. A background check typically costs around \$25 for the most basic level to around \$60 for a more thorough scan, DeLoach says.

“Some states will require only that the provider conduct a state-specific criminal background check, which is OK as far as that goes,” she says. “But if you think about someone who has lived in several states and jurisdictions, perhaps only recently moved to your state, they may not have a record that would show up in that screening.”

The better option would be to do a seven-year criminal search nationwide rather than just the minimum required by the state, she says.

“People with criminal records or other problems know that it will be a problem in hiring, so they do their research. They’re wise about the laws and what kind of screening takes place,” DeLoach explains. “They move to get a fresh start and hope, or sometimes they’ve researched it and know, that you will only look so far.”

Ongoing screening also needed

DeLoach points out that for health care providers, the quality of the staff can be the facility’s brand. Many hospitals market their staff as exceptional, making them the “face” of the organization and a key drawing point for patients who can choose among facilities for delivering babies or other care. If an employee commits a crime and that incident is publicized by the media, that marketing effort stalls and the organization can suffer a significant downturn in business, she says.

Criminal records are not the only concern, of course. Background checks can include screening for changes to a physician or other professional’s credentials, such as disciplinary actions. Some regulatory agencies require periodic checks of physician credentials, DeLoach notes.

Ongoing screening also can be important after the employee is hired or the physician is granted privileges, DeLoach says. Some states require a periodic check for any new criminal charges, but DeLoach says it is a good idea even if it is not required. Many providers conduct an annual screening of the entire employee population, she says.

“We also can do a payroll screening in which we draw off the names of every employee from the payroll data and compare that to our background screening records, not necessarily to do a new background check on everyone, but to ensure that everyone has already been screened at some point,” DeLoach says. “We want to make sure that everyone has been checked and no one missed that step for some reason, such as employees being

merged from another organization.”

Be wary of false credentials

Remember that background checks should involve more than criminal records. Risk managers should encourage a healthy degree of skepticism in anyone involved in recruiting, interviewing, and hiring staff, says **Jeff Wizeb**, vice president for business development with screening company HR Plus, a division of AlliedBarton Security Services, based in Chicago.

In today’s competitive employee market, up to 70% of applicants include false information on their resumes and job applications, he says. As a result, many companies may hire the wrong individual, who could possibly damage the reputation of the company with one incident.

“There are more and more fake job reference sites springing up on the Internet, where users can pay to have falsified references sent to prospective employers,” Wizeb says. “It is becoming a larger human resources issue, much like the emergence of the fake college degrees in the past.”

A thorough background check can help protect the provider if the employee’s actions prompt a lawsuit, Wizeb says.

“You can bring out your documentation showing that you acted in good faith and obtained a good background check on this person, looking for any indication he was going to pose a risk,” Wizeb says. “Maybe something still happened with that person, but you can show that you did your due diligence; and there were no red flags suggesting that this person was a danger and that you should have known when you hired him.”

Wizeb points out that the provider’s employees are not the only concern. Contractors and other third parties often have the same access to patients, drugs, and data that employees have, or sometimes even more access. Risk managers should ensure that those people are being properly screened by their employers, Wizeb says.

Be known for tough screening

The need to screen employees is particularly acute with home health workers and similar staff who have extensive access to patients, says **Pernille Ostberg**, president of Matrix Home Care in West Palm Beach, FL, which employs health care workers and services clients in 30 counties throughout the state of Florida.

Telephone: (773) 864-2387. E-mail: jwizceb@hrplus.com.

• **Pernille Ostberg**, MBA, RPH, President, Matrix Home Care, West Palm Beach, FL. Telephone: (888) 806-9040. ■

Tips for improving background checks

Pernille Ostberg, president of Matrix Home Care in West Palm Beach, FL, offers these tips for improving background checks on health care workers:

- Educate yourself on the different types of screening. Are checks being done on a national, statewide, or local level? Is there a review of prior arrests and convictions, including motor vehicle tickets and accidents?
- When hiring from an agency, discuss the agency's screening policies and procedures. Don't just accept their assurance that they do background checks. Find out exactly how they are conducted. Do they check for the past year? Seven years? Misdemeanors? Just felonies?
- Don't accept a candidate's copy of a prior background screening. It could have been changed or forged.
- Validate any information relating to a potential issue, such as a pending divorce or home foreclosure. Don't assume the facts are correct until they can be verified.
- Ask for references, and be sure to talk with them. This can be the most important part of a background check. References may reveal information that is not apparent in the background check documentation. ■

HIEs create privacy issues for providers

Health information exchanges (HIEs), which support secure electronic sharing of patient health information among caregivers, patients, public health authorities, and health care and payment services providers across different setting and geographical areas, are among the most promising initiatives in health care, but there are privacy and security issues that should concern risk managers.

On a large scale, HIEs make it possible to cre-

“From my perspective, based on 30 years in the home care industry, there's simply no substitute for screening out the bad apples before they get into the system,” she says. “And, of course, any caregiver found to be involved in criminal behavior should be turned in to the police immediately.”

Ostberg points out that any negative incident with an employee, such as criminal behavior or charges of abuse or fraud, should prompt the organization to go back and look at how that person was hired. The review may reveal weaknesses in your background screening process, such as a criminal history that could have been found if the check has been more extensive, she says.

Ostberg personally reviews every background check before an employee is hired. She advocates extremely thorough screening, because over the years she has seen links between seemingly innocuous behavior in a person's record and subsequent malfeasance on the job. For instance, Matrix studies a person's driving record, even if the person will not be driving on the job. (See page 68 for more tips on screening.)

“A bad background screen is often mirrored in the driving record. We can see that a history of driving infractions, things like failing to use a turn signal or speeding, can correlate to an employee who is going to be a problem for us later on,” she says. “A lot of traffic stops on the record can mean there is more going on than just what the person ultimately got a ticket for, and it can sometimes reveal red flags like being combative with the police.”

Ostberg notes that people with questionable backgrounds seek out the facilities that do not conduct thorough checks. If your organization becomes known as the provider that is lax in screening, your risk of hiring people with bad backgrounds will skyrocket, because those people are drawn to you and can't get hired elsewhere, she says.

“Whenever we open a new facility in a community, we are inundated by applicants with bad backgrounds,” she says. “They're checking to see if we screen people thoroughly, and once word gets out that we do, those people stop applying.”

SOURCES

For more information on background checks, contact:

- **Jenifer DeLoach**, Senior Vice President, Kroll, Nashville, TN. Telephone: (615) 320-9800, ext. 20559.
- **Jeff Wizceb**, Vice President Business Development, HR Plus, A Division of AlliedBarton Security Services, Chicago.

ate a nationwide health information infrastructure through which providers can access any patient data that they need, regardless of location. The Health Information Technology for Economic and Clinical Health (HITECH) Act provides up to \$36 billion of financial incentives to providers for using electronic health records that have the capability to support HIE through “meaningful use.” The HITECH Act also gives more than \$300 million in funding to regional or local health IT efforts and instructs the Health and Human Services Secretary to invest in the infrastructure necessary to enable the electronic exchange and use of health information for each individual.

But the benefits of HIEs can only be as good as the patients’ willingness to share their health information, and some are reluctant to participate, since this level of sharing can increase the risks of unauthorized access to information, says **Jared Rhoads**, senior research analyst with CSC, a technology consulting company based in Falls Church, VA. Without patient trust and consent to share data, the usefulness and sustainability of an HIE is severely undermined, making privacy and security critical to its success, Rhoads says.

“Ensuring privacy is a challenge when you’re talking about something like an HIE, which is premised on the idea of giving someone a person’s personal health information, but providers are addressing the challenge; and we’re seeing that they’re coming up with solutions that work [for] them,” Rhoads says. “They are drawing on the experience they’ve had with HIPAA to develop ways to make that information useful and still make sure that it doesn’t get misused or used in a way for which the patient did not give permission.”

The key benefit of an HIE is the ability to send and request health information. An authorized physician can access a patient’s medical history

EXECUTIVE SUMMARY

More providers are becoming involved with health information exchanges, and risk managers must consider issues of liability and patient privacy. The applicable laws are complex and sometimes seem contradictory.

- Providers will need to obtain patient consent.
- Documentation of information-sharing paths can help if data are misused.
- Experience with HIPAA can be applied to the development of exchanges.

and obtain a list of current medications, known allergies, and other vital information, regardless of where it was originally recorded, Rhoads says. To make the systems secure and win the trust and consent of patients, Rhoads says health care organizations must take these steps:

- Determine which data to share and how to share them.
- Develop practices to manage authorized access.
- Adopt policies and practices to prevent unauthorized access.
- Gain informed consent from patients.
- Be prepared to address breaches.

HIPAA may be revised

Some caution is warranted when establishing or joining an HIE, but providers should be careful not to focus excessively on privacy concerns, says **Greg DeBor**, client partner for health delivery with CSC, who developed and oversaw the New England Healthcare Exchange Network (NEHEN), a consortium of regional payers and providers that includes 55 hospitals, eight health insurance plans, and tens of thousands of practitioners. NEHEN started in 1998, first with only administrative data and then clinical data also, and it is one of longest-running HIEs in the country.

DeBor notes that implementation of HIEs can be hampered by concerns over how to share data while still meeting the privacy and confidentiality requirements in the Health Information Portability and Accountability Act (HIPAA). Much of that concern is justified, he says, but it is clear that the government wants to encourage HIEs and won’t let HIPAA stand in the way. With providers wondering how they can comply with HIPAA and still meet the goals of an HIE, DeBor says there likely will be changes to HIPAA to address those problems.

“The privacy section of HITECH says that the federal government will have to tighten up some things that were first specified in HIPAA to make these HIEs possible,” he says. “First, there has to be a much more [prescriptive] definition of what constitutes operations, because HIPAA allows sharing of data if it’s related to payment, treatment, and operations, but the operations part of that has been loosely interpreted by the industry. Also, the government needs to hire a chief privacy officer for the nation and to give the industry more guidance on privacy and security.”

Risk managers involved in developing an HIE should consult with the business side of the health care operation to understand what kind of data requests are received from business partners, DeBor says. The meaningful use policy requires that the provider share significant amounts of data to earn incentives, but the types of data will vary from one provider to the next, he says.

Another issue involves consent from patients. If HIPAA is refined to indicate that HIE data is included in the “operations” definition, consent may not be as necessary, but as the law stands, it appears that each patient will need to consent to having data included in the exchange, DeBor says. (For more on obtaining consent for an HIE, see below.)

“Making patient data available to others opens up a lot of questions about how that data is used and who will be responsible if it is misused. If you exchange data and that data is misused by someone else down the line, are you liable?” DeBor says. “You had better be able to document your disclosures, at least, so that you can document who you shared data with and create an audit trail on that. That’s one place to start when looking at liability issues, building that into the system and taking into consideration with the design of the exchange.”

[CSC has made a white paper on HIE confidentiality and security available on its website at no charge. Go to www.csc.com/health_services/insights/30034-hitech_s_impact_on_health_information_exchanges_key_decision_points_for_privacy_and_security.]

SOURCES

For more information on HIEs, contact:

- **Jared Rhoads**, Senior Research Analyst, CSC, Falls Church, VA. Telephone: (781) 290-1740. E-mail: jrhoads@csc.com.
- **Greg DeBor**, Client Partner for Health Delivery, CSC, Falls Church, VA. Telephone: (781) 290-1308. E-mail: gdebor@csc.com. ■

Work early to gain consent of patients

Gaining patient consent and provider adoption for health information exchanges (HIEs) is important for the success of the effort, and

patients must be adequately educated about the HIE or they may not give their permission, says **Jared Rhoads**, senior research analyst with CSC, a technology consulting company based in Falls Church, VA.

The information provided to patients should explain the purpose, benefits, and risks of data sharing, so patients make informed decisions, he says. This includes understanding what information is being shared across the exchange, which organizations are participating, what safeguards have been put in place to protect their privacy, who can access and use the information, and where the data reside.

Rhoads notes that education to gain community support can take a number of forms. Printed materials, direct mailings, and even paid advertising can be effective. Some HIEs post informational videos online or sponsor kickoff events that are open to the public. As part of its consumer education campaign, the Vermont Information Technology Leaders (VITL) health exchange showcased the fact that VITL’s standards for privacy and security exceed those used by the federal government, Rhoads says.

Physicians can have great impact on the education process and can encourage patients to trust the security of the HIE, he says.

“Patients usually trust their physician, and that dialogue between the doctor and the patient can be one of the most effective ways to tell patients what the HIE is all about, how it works, and why it’s a good idea to participate,” Rhoads says. “Getting the physicians on board and enthusiastic can be very beneficial if they are then willing to talk with their patients and tell them why the HIE will benefit and why they should consent.”

Advance notice of the HIE also is important. No one likes to be surprised by a big project that involves their sensitive data. Rhoads points out that when patients in the United Kingdom were notified of an HIE project in development and given plenty of time to learn about it, almost everyone consented. But when patients in the Netherlands were informed about an HIE at the last minute, just before the system was ready to go, they did not respond well to the letters asking for permission. They balked, with many refusing and others sending incomplete information in response, which led to a significant delay in starting the HIE, Rhoads says.

Rhoads notes that the patient does not have to consent to any and all transmission of personal

health data. Some flexibility is acceptable and can encourage higher rates of consent. For instance, the HIE may offer patients the ability to allow access to data only for emergencies, or to allow or disallow data from certain sources.

“It doesn’t have to be all or nothing,” he says. “It’s better to have a lot of people consent to using the data in some ways than to have them all decline because there were some types of data or some specific uses that they objected to.” ■

Health worker gets prison for peeking at records

A former University of California-Los Angeles (UCLA) Healthcare System employee who says he had no idea it was a crime to look at patient records will have four months in prison to think about it.

United States Magistrate Judge Andrew J. Wistrich, JD, recently sentenced Huping Zhou, 47, of Los Angeles, to four months in federal prison, apparently making him the first person ever sent to prison for violating privacy laws but not using the information for other illegal activity, such as identity theft. The judge condemned Zhou for his lack of respect for patient privacy. Zhou admitted to illegally reading private and confidential medical records, mostly from celebrities and other high-profile patients, but a statement from the U.S. Attorney’s office in Los Angeles says there is no evidence that Zhou improperly used or attempted to sell any of the information that he illegally accessed.

Zhou pleaded guilty in January 2010 to four misdemeanor counts of violating the federal privacy provisions of the Health Insurance Portability and Accountability Act (HIPAA). Zhou specifically admitted to knowingly obtaining individually identifiable health information without a valid reason, medical or otherwise, according to the U.S. Attorney’s office.

The U.S. Attorney’s office provides this description of the crime: Zhou, who is a licensed cardiothoracic surgeon in China, was employed in 2003 at UCLA Healthcare System as a researcher with the UCLA School of Medicine. On Oct. 29, 2003, Zhou received a notice of intent to dismiss him from UCLA Healthcare for job performance

reasons unrelated to his illegal access of medical records. That night, Zhou, without any legal or medical reason, accessed and read his immediate supervisor’s medical records and those of other co-workers. For the next three weeks, Zhou’s continued his illegal accessing of patient records and expanded his illegal conduct to include confidential health records belonging to various celebrities. According to court documents, Zhou accessed the UCLA patient records system 323 times during the three-week period, with most of the accesses involving well-recognized celebrities.

In his plea agreement, Zhou admitted that he obtained and read private patient health and medical information on four specific occasions after he was formally terminated from the UCLA Healthcare System. Zhou acknowledged that at the time he viewed these patients’ medical information, he had no legitimate reason, medical or otherwise, for obtaining the personal information. ■

CNE OBJECTIVES

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

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

COMING IN FUTURE MONTHS

■ Identifying adverse events

■ Career tips for risk managers

■ RAC audit lessons

■ More on effects of health reform

EDITORIAL ADVISORY BOARD

Maureen Archambault RN, CHRM, MBA Senior Vice President, Healthcare Practice Leader Marsh Risk and Insurance Services Los Angeles	Leilani Kicklighter RN, ARM, MBA, CPHRM LHRM Patient Safety & Risk Management Consultant The Kicklighter Group Tamarac, FL
Jane J. McCaffrey MHSA, DFASHRM Director Safety and Risk Management Self Regional Healthcare Greenwood, SC	John C. Metcalfe JD, FASHRM Vice President Risk Management Services Memorial Health Services Long Beach, CA
Sandra K.C. Johnson RN, ARM, FASHRM Director, Risk Services North Broward Hospital District Fort Lauderdale, FL	Grena Porto, RN, MS, ARM, CPHRM Senior Vice President Marsh Philadelphia
R. Stephen Trosty JD, MHA, CPHRM Risk Management Consultant Haslett, MI	

To reproduce any part of this newsletter for promotional purposes, please contact:

Stephen Vance

Phone: (800) 688-2421, ext. 5511

Fax: (800) 284-3291

Email: stephen.vance@ahcmedia.com

To obtain information and pricing on group discounts, multiple copies, site-licenses, or electronic distribution please contact:

Tria Kreutzer

Phone: (800) 688-2421, ext. 5482

Fax: (800) 284-3291

Email: tria.kreutzer@ahcmedia.com

Address: AHC Media LLC
3525 Piedmont Road, Bldg. 6, Ste. 400
Atlanta, GA 30305 USA

To reproduce any part of AHC newsletters for educational purposes, please contact:

The Copyright Clearance Center for permission

Email: info@copyright.com

Website: www.copyright.com

Phone: (978) 750-8400

Fax: (978) 646-8600

Address: Copyright Clearance Center
222 Rosewood Drive
Danvers, MA 01923 USA

CNE QUESTIONS

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

21. How was the theft of 370,000 pills from The Parkland Health and Hospital System of Texas discovered?

- A. The State Board of Pharmacy reported irregularities to the hospital system.
- B. Local police traced illegal narcotics back to the hospital pharmacies.
- C. The Drug Enforcement Administration detected a high rate of narcotic prescriptions.
- D. The Parkland Health and Hospital System discovered the thefts on its own.

22. According to research conducted by Maria Rosario Gonzales, RN, a nurse educator in the Veterans Administration Healthcare System in Los Angeles, what was one problem with the response to missing patients at her facility?

- A. The lack of unit or ward specific search grids slowed the response and caused the preliminary search to be inefficient and ineffective.
- B. Staff delayed their response in hopes the patient was not in danger.
- C. The response was delayed because staff had to seek approval from superiors before initiating a search.
- D. Some staff refused to participate in searches for missing patients.

23. What does Jenifer DeLoach, senior vice president with Kroll, a risk consulting firm in Nashville, TN, advise regarding background checks?

- A. Do whatever is required by state law but don't spend money on more.
- B. Do only a state-specific criminal background check.
- C. There is no need to do background checks on most employees.
- D. Do extensive background checks, as thorough as your budget will allow.

24. According to Jared Rhoads, senior research analyst with CSC, a technology consulting company based in Falls Church, VA, what is the best way to obtain patient consent for a health information exchange (HIE)?

- A. Begin educating and seeking consent early in the development process.
- B. Wait until the HIE is nearly operational and then seek consent.
- C. Ask for consent after the HIE is operational but before any patient data are exchanged.
- D. Ask for consent when the first request for that patient's data is received.

Answers 21. D; 22. A; 23. D; 24. A