HEALTHCARE RISK MANAGEMENT™

THE TRUSTED SOURCE FOR LEGAL AND PATIENT SAFETY ADVICE FOR MORE THAN THREE DECADES

INSIDE

RELIAS
Formerly AHC Media

MARCH 2018 Vol. 40, No. 3; p. 25-36

Hospital Takes Safety Score From 'C' to 'A' With Targeted Improvements

Two hospitals in Wisconsin undertook a concerted effort to improve patient safety after receiving a "C" from The Leapfrog Group, raising their scores to an "A" over two years.

Hospital Sisters Health System (HSHS) Sacred Heart Hospital in Eau Claire, and St. Joseph's Hospital in Chippewa Falls, both received the top rating recently from The Leapfrog Group, a national nonprofit healthcare ratings organization that assigns letter grades to hospitals nationwide based on performance in preventing medical errors, infections, and other harm.

The Leapfrog Hospital Safety Grade uses 27 measures of publicly available hospital safety data to assign grades to more than 2,600 U.S. hospitals twice per year. The grades are assessed by patient safety experts and are peer-reviewed.

> "EVERY HOSPITAL RUNS INTO THE TENDENCY TO DRIFT AWAY FROM THE PROCESS, SO YOU HAVE TO ACCEPT THAT AND HAVE A SYSTEM IN PLACE TO DISCOURAGE THAT AND SPOT IT WHEN IT HAPPENS."

The hospitals both scored a "C" in 2015 and an "A" in the spring of 2017, says **Tammy Lampro**, MT, MBA, CQE(ASQ), patient safety officer at both hospitals. That improvement required several interventions, she says.

"The grade is based on how each hospital performs against the other hospitals across the nation at that time, so it is a bit of a moving target. You can't say this was the level to achieve in 2015 and carry

Financial Disclosure: Author **Greg Freeman**, Editor **Jill Drachenberg**, Editor **Jesse Saffron**, Editorial Group Manager **Terrey L. Hatcher** 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. Consulting Editor **Arnold Mackles**, MD, MBA, LHRM, discloses that he is an author and advisory board member for The Sullivan Group and that he is owner, stockholder, presenter, author, and consultant for Innovative Healthcare Compliance Group.

HEALTHCARE RISK MANAGEMENT™

Healthcare Risk Management™,
ISSN 1081-6534, including *Legal Review & Commentary*™
is published monthly by
AHC Media, LLC, a Relias Learning company
111 Corning Road, Suite 250
Cary, NC 27518

Periodicals Postage Paid at Cary, NC, and at additional mailing offices
GST Registration Number: R128870672

POSTMASTER: Send address changes to: *Healthcare Risk Management*
Relias Learning
111 Corning Road, Suite 250
Cary, NC 27518

SUBSCRIBER INFORMATION: Customer Service: (800) 688-2421. Customer.Service@AHCMedia.com
AHCMedia.com

SUBSCRIPTION PRICES: USA, Print: 1 year (12 issues) with free CE nursing contact hours and free *AMA PRA Category 1 Credits*™, $519. Add $19.99 for shipping & handling. Online only, single user: 1 year with free CE nursing contact hours and free AMA PRA Category 1 Credits™, $469. Outside USA, add $30 per year, total prepaid in USA funds.

MULTIPLE COPIES: Discounts are available for group subscriptions, multiple copies, site licenses, or electronic distribution. For pricing information, please contact our Group Account Managers at Groups@AHCMedia.com or (866) 213-0844. 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.)

ACCREDITATION: Relias Learning, LLC, is accredited as a provider of continuing nursing education by the American Nurses Credentialing Center's Commission on Accreditation. Contact hours [1.5] will be awarded to participants who meet the criteria for successful completion. California Board of Registered Nursing, Provider CEP#13791.

Relias Learning is accredited by the Accreditation Council for Continuing Medical Education (ACCME) to provide continuing medical education for physicians. Relias Learning designates this enduring material for a maximum of 1.5 *AMA PRA Category 1 Credits*™. Physicians should claim only credit commensurate with the extent of their participation in an activity.

Healthcare Risk Management™ is intended for risk managers, healthcare administrators, healthcare legal counsel, and physicians. This activity is valid 36 months from the date of publication.

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.

AUTHOR: Greg Freeman
EDITOR: Jill Drachenberg
EDITOR: Jesse Saffron
EDITORIAL GROUP MANAGER: Terrey L. Hatcher
SENIOR ACCREDITATIONS OFFICER: Lee Landenberger

EDITORIAL QUESTIONS
Call Editor **Jill Drachenberg**, (404) 262-5508

that forward, because everyone else is improving at the same time," Lampro says. "We're always looking to improve our processes and be better every day, so this was an opportunity to look at what could be changed."

The hospitals targeted several areas in which patient safety could be improved. One was reducing the incidence of retained surgical items (RSIs), so the hospitals adopted the NoThing Left Behind program (http://www.nothingleftbehind.org), particularly the rigorous sponge accounting process.

"This was a more thorough, standardized process than what we were doing before, and we now have a policy that if the count is off we always do an X-ray and make sure it is not in the patient," Lampro explains. "The Leapfrog data gives you a starting place to see what happened and then you have to investigate to see what object was retained and how you could prevent that from happening in the future. It's root-cause analysis and continuous process improvement, with your past experience as a guide to where you should devote time and resources."

HAIs Also Targeted

Another effort involved reducing hospital-acquired infections (HAIs) such as catheter-associated urinary tract infections (CAUTIs), central line-associated bloodstream infections, and surgical infections. The hospitals made an effort to follow the established best practices for reducing these infections, including not leaving catheters in any longer than necessary.

Following the best practices to the letter every time, every day was the goal, Lampro says.

"Every hospital runs into the tendency to drift away from the process, so you have to accept that and have a system in place to discourage that and spot it when it happens. You also have to stay on top of training new people when they come in," Lampro says. "That's a constant management challenge."

Implementing best practices is not always an easy task, Lampro says. The hospitals found that although a best practice may be accepted by the clinical community, your own clinicians may still want to know why it is better than what they are currently doing.

"We addressed that partly by bringing people into the process early, helping them understand what we're moving to and exactly what it entails. A lot of times, resistance comes from just not fully understanding what someone is asking you to do, and you can dispel that by showing them," Lampro says. "For example, the CAUTI best practices call for a kit you use with the cleaning products and everything else you need. Before we adopted it, we talked to everyone involved to

EXECUTIVE SUMMARY

Hospitals improved poor Leapfrog scores with a series of interventions. One strategy involved an ultraviolet sterilization system.

- Expect some resistance to adopting best practices.
- Retained surgical items also were targeted.
- Clinicians may drift away from established policies and procedures.

really get their engagement up front, and we piloted it on some areas before we moved forward in a bigger way."

The hospitals also eliminated unnecessary traffic in the OR and improved cleaning processes in the hospital, says **Sue Galoff**, RN, MHA, infection prevention manager at HSHS Sacred Heart and St. Joseph's hospitals. One of the cleaning process improvements was the addition of an ultraviolet light sterilization system.

The system uses short-wavelength ultraviolet (UVC) light to kill or inactivate microorganisms on surfaces in the room, explains **Steven Wheeler**, CHESP, director of environmental services at HSHS Sacred Heart and St. Joseph's hospitals. The light destroys nucleic acids and disrupts the DNA of microorganisms, leaving them unable to perform vital cellular functions.

A large, randomized trial led by Duke Health found that UVC machines can cut transmission of four major superbugs by a cumulative 30%. The trial included more than 21,000 patients at nine hospitals in the Southeast, including three Duke University Health System hospitals, a Veterans Affairs hospital, and small community healthcare settings. It focused on patients staying overnight in a room where the previous patient was known to have an infection from a drug-resistant organism: methicillin-resistant *Staphylococcus aureus* (MRSA), vancomycin-resistant enterococci (VRE), *Clostridium difficile*, and *Acinetobacter*. (*An abstract of the study is available online at: http://bit.ly/2k3s3B8.)*

"We started with our *C. difficile* isolation rooms because it is effective on the *C. diff* spores, but our ultimate goal is to do it with every single discharge so we have that added assurance that any HAIs are taken care of," he says.

The cost of the UVC system was significant, so they had to make the case that the patient safety improvements would be worth the expense both in the savings of real dollars from fewer HAIs and in the less tangible benefits to patient care. UVC systems are available for hospital use from several manufacturers, and a single unit can cost around $90,000.

"It also is a time-consuming process, so it adds to the turnaround time for that room. That means we have to make sure we're using best practices for the procedure and maximizing the amount of time we have to clean the room and add that disinfection time," Wheeler says. "Sometimes, it is not enough to have the technology and tell people to use it. You have to put some thought into the best ways to use it efficiently."

> "IF YOU'RE AN ORGANIZATION LOOKING AT WHERE TO START IMPROVING PATIENT SAFETY, TARGETING BASED ON DATA IS A GOOD STRATEGY."

The UVC operates on line of sight, so the unit must be activated in more than one spot in a room to make sure everything has been covered. For a typical patient room, the sterilization requires three placements for five minutes each.

"It took us a while to work that into our bed turnaround process and figure out how to be effective with it," Wheeler says. "For instance, we figured out that we could save time by shooting the bathroom first, putting the unit in the bathroom with the door closed while the housecleaner cleans the rest of the room. We wanted to reduce the HAIs without unnecessarily holding up the process of making that bed available to the next patient."

The hospitals also had to add new staff positions in environmental services to accommodate the extra steps for cleaning.

The investment in the technology and additional staff were justified by the reduction in infections that the hospital is seeing, Galoff says.

"If you're an organization looking at where to start improving patient safety, targeting based on data is a good strategy. The data leads you to look at where you should focus, and for us that was the *C. diff* area," she says. "A lot of work goes into all of these processes, but you can start small, with pilot projects and then expanding to your most vulnerable areas and finally going as wide within the organization as you want." ■

SOURCES

- Sue Galoff, RN, MHA, Infection Prevention Manager, Hospital Sisters Health System Sacred Heart Hospital, Eau Claire, WI, and St. Joseph's Hospital, Chippewa Falls, WI. Email: sue.galoff@hshs.org.
- Tammy Lampro, MT, MBA, CQE(ASQ), Patient Safety Officer, Hospital Sisters Health System Sacred Heart Hospital, Eau Claire, WI, and St. Joseph's Hospital, Chippewa Falls, WI. Email: tammy.lampro@hshs.org.
- Steven Wheeler, CHESP, Director of Environmental Services, Hospital Sisters Health System Sacred Heart Hospital, Eau Claire, WI, and St. Joseph's Hospital, Chippewa Falls, WI. Email: steven.wheeler@hshs.org.

Red Light Says 'Not Now' for Nurses in Critical Work

Nurses have a lot of responsibilities and must sometimes perform several tasks at once, but there are times when their full attention is needed for a task that is critical to patient safety. One hospital is using red lights on workstations to indicate that the nurse must not be interrupted.

The idea came out of a patient safety committee that focuses on adverse drug events, says **Bonnie Seitz**, MS, RN, CPN, CNS, pediatric safety officer at Upstate Golisano Children's Hospital in Syracuse, NY. Staff had seen clinicians at other hospitals using lights on their hospital identification lanyards to indicate that they should not be interrupted, and the idea grew from there.

Organizations including the Institute for Safe Medication Practices and the Agency for Healthcare Research and Quality, as well as other nursing groups, have recommended strategies aimed at increasing clinicians' focus on tasks particularly vulnerable to mistakes, such as determining medication dosages.

The hospital tried other strategies, including "no interruption" zones in the unit, indicators on lanyards, pins on the uniform, and vests indicating no one should talk to the wearer. When considering the options, Upstate Golisano staff were interested in the idea of a red light on the ceiling that the nurse could activate when preparing medications on a WOW, a workstation on wheels. But that would require going to that space specifically for the task.

> "WE ALSO PUT SIGNS UP IN ALL THE CHARTING AREAS FOR PHYSICIANS TO TELL THEM, 'WHEN YOU SEE THESE LIGHTS ON, DON'T INTERRUPT THE NURSES.'"

"We thought about it more and decided we needed something that would work when we push the med cart into the patient room, because a lot of times the nurses are giving the medications right off the medication cart at the bedside," Seitz says. "Gone are the days when you had a medication room, where you fixed all your meds up and brought them on a tray to the patient's room."

Now, nurses take the meds from a medication dispensing unit, put them on a WOW, and enter the patient's room to perform the critical medication checks and administer them. The hospital settled on a solution that involved attaching a red light to the WOW, along with a sign that says, "What does the red light mean? Please don't interrupt me. I need to focus to keep my patients safe."

Nurses also explain while orienting patients and family to the room that the red light indicates a no-interruption zone.

"We also put signs up in all the charting areas for physicians to tell them, 'When you see these lights on, don't interrupt the nurses,'" Seitz says.

Inexpensive to Implement

Upstate Golisano implemented the system in December 2017, paying $425 for the LED lights and Velcro to attach them. The hospital first obtained samples of a few different kinds of lights and took them out on the units to get nurses' feedback on which ones they liked and how to place them on the carts.

To avoid blinding the user or people nearby, the lights are faced up toward the ceiling.

The red lights are available for all nurses, but about half have not warmed to the idea yet, she says. The reasons Seitz hears from nurses include doubts that anyone will honor the red light and not interrupt,

EXECUTIVE SUMMARY

Red lights at nursing workstations can improve patient safety. The lights signal others not to interrupt during critical work.

- No-interruption zones help clinicians avoid errors, particularly with medication.
- The system was implemented with little expense.
- All staff, patients, and family must be educated about what the light means.

and concerns about looking out of step by using the light when other nurses on the unit don't.

"I try to push the evidence and impress on them there is lots of proof that this works," Seitz says. "If we all come on board and use it, this becomes part of our culture that when you see that red light on, that means you don't interrupt the nurse. If you hold people accountable, it will become embedded and it will become known that that's how things work in the children's hospital: A red light means you don't interrupt."

The pharmacy director now has adopted the idea, installing red lights in two work areas where he doesn't want pharmacy technicians interrupted. Respiratory therapists also have expressed interest in placing red lights on their carts.

"Making changes in a busy work environment can be challenging, but we've been on this journey since 2009 to change the culture of safety at our hospital," she says. "Just introducing a good idea doesn't mean it's going to catch on immediately, but this one is gaining popularity and we're not going to let it go because there is so much good evidence for no-interruption zones." ■

SOURCE

- Bonnie Seitz, MS, RN, CPN, CNS, Pediatric Safety Officer, Upstate Golisano Children's Hospital, Syracuse, NY. Phone: (315) 464-5437.

Nurse Sues Health System for Firing After Safety Complaints

A hospital and health system in California is facing a lawsuit from a nurse who says she was fired for blowing the whistle on unsafe working conditions that threatened patients and staff.

Teresa Brooke, former chief nursing officer (CNO) at Aurora Santa Rosa Hospital, an acute psychiatric facility in Sonoma County operated by Aurora Behavioral Healthcare and Signature Healthcare Services, says she only wanted a safe environment for her staff and patients. Her lawsuit alleges the health system was more concerned about profits than dangerous conditions at the hospital.

Severe staff shortages resulted in injuries to patients and staff during her time as CNO, she claims. The facility provides inpatient, partial hospitalization, and outpatient mental health services to adults and adolescents.

Brooke had 30 years' experience in nursing and hospital management before joining the Aurora facility, according to her attorney **Xinying Valerian**, JD, of Valerian Law in San Francisco. Brooke raised her concerns both internally and to a government agency, and was summarily fired, Valerian says.

Lawsuit Alleges Dangerous Conditions

She is seeking general economic and noneconomic damages, special damages, punitive damages, permanent injunctive relief, legal fees, pre- and post-judgment interest, and other relief the court may find appropriate. The health system did not respond to a request for comment.

Her whistleblower lawsuit alleges wrongful termination and retaliation in violation of several provisions of the California Labor and Health and Safety Codes.

The complaint details numerous examples of dangerous conditions at the hospital, including severe staff shortages that resulted in injuries to patients and staff. Brooke claims that Aurora and Signature illegally fired her for complaining about those conditions.

The case illustrates the elevated risk that comes from mishandling the sometimes inevitable clash of business and clinical priorities, Valerian says.

"Teresa Brooke is an experienced nurse and manager, but what she saw at this facility was worse than anything she had seen before, and she was rightly concerned," Valerian says. "There is inherent risk in

EXECUTIVE SUMMARY

A nurse is suing the health system that fired her after complaints about patient and staff safety. She claims wrongful termination.

- The nurse claims the behavioral health facility was understaffed.
- Patients and staff were harmed as a result, she says.
- The nurse reported her concerns to a state agency and then was fired.

overriding the judgment of your top clinical leaders and allowing business decisions to interfere with clinical and safety decisions. It is appropriate to set business goals for your facility, of course, but problems come when the business side gets involved at the granular level day to day."

Violence, Self-harm, Sexual Abuse

The complaint alleges that staff and patients "were subjected to routine punching, kicking, choking, and, on one occasion, even a full-blown patient riot" and that the staffing shortages "led to high incidence of patient self-harm and multiple occurrences of sexual violence involving patients, some of them minors."

Aurora and Signature prioritized profits over the care and rights of patients and hospital staff , the lawsuit claims. Brooke tried to limit admissions and increase staffing, but met resistance from corporate leaders, she says. Instead of respecting her admissions caps and limits on after-hours admissions when on-duty staffing was inadequate, the health system decided to open an additional patient unit.

"When you're talking about staffing concerns, you can't separate concerns [about] the safety of workers and the safety of patients. They're all intertwined," Valerian says. "Inadequate staffing put them all in harm's way."

Brooke filed a complaint about understaffing and unsafe conditions with the California Department of Public Health (CDPH) in fall 2016 and says she was fired without warning soon after.

CDPH investigated Brooke's complaints and "substantiated and validated" them, according to the lawsuit.

Fired After Reporting Concerns

The complaint alleges numerous California Labor Code and OSHA violations, including chronic understaffing, unsafe placement of patient seclusion and restraint rooms, unsafe administration of medications, failure to provide sufficient hand-washing and sanitizing stations, lack of a workplace injury and illness prevention program for employees, failure to provide staff with suitable seating, and illegal confidentiality policies and practices for employees. *(See the story below for excerpts from the complaint.)*

The complaint cites nine causes of action, including wrongful termination, retaliation in violation of several provisions of the California Labor and Health and Safety Codes, solicitation of an employee by misrepresentation in violation of the California Labor Code, and a private attorney general enforcement claim.

"My client was fired only a few weeks after she went to the state public health department, and there was no replacement lined up to fill this critical leadership role. So, from a lawyer's perspective, the closeness in time between a protected activity such as filing a complaint with the authorities and the adverse employment action was a critical factor in determining the strength of this case," Valerian says. "She had no warning, a positive performance review a couple of weeks prior, so there nothing to substantiate the termination." ■

SOURCE

- Xinying Valerian, JD, Valerian Law, San Francisco. Phone: (888) 686-1918. Email: contactus@valerian.law.

Former CNO Alleges Understaffing, Violence at Psychiatric Hospital

In her lawsuit against Aurora Santa Rosa Hospital, an acute psychiatric facility in Sonoma County, CA, operated by Aurora Behavioral Healthcare and Signature Healthcare Services, former chief nursing officer Teresa Brooke alleges she was fired for complaining about unsafe conditions for patients and staff.

"Plaintiff arrived at the hospital to find dangerous conditions unlike anything she had encountered in her 30 years of nursing. Running on a shoestring budget from corporate leadership at Signature, the hospital was plagued by a high incidence of injuries resulting from understaffing of the skilled nurses and other caregivers needed to care for high-needs patients," according to the complaint. "While the overriding goal of clinicians like plaintiff was 'safety first,' the company's overriding concern was increasing patient census (or, headcount) and minimizing costs. For the company, profits came first and patients dead last."

The lawsuit claims that outdated practices long abandoned by the psychiatric community flourished at the hospital, including the "warehousing" of patients who were "left with little to do other than pace up and down the halls of the unit or sit in front of a television. There were not enough staffers to provide anything but the most basic supervision, and sometimes not even that."

Underpaid and overworked staff nurses and mental health workers faced repeated violent outbreaks among patients, the lawsuit claims. Staff and patients were subjected to routine punching, kicking, choking, and patients even rioted at one point, Brooke claims. Patients, including minors, also were subject to a high incidence of patient self-harm and sexual violence because staffing was too low to adequately supervise them, the lawsuit claims.

In October 2016, the company abruptly fired Aurora's chief executive officer, who had supported Brooke's recommendations, including postponing the opening of the new unit and capping admissions, the lawsuit claims. The company appointed its chief financial officer as interim CEO.

"Seeing the futility of her internal resistance and fearing that the new unit would open before staffing levels could support it, plaintiff complained to the California Department of Public Health (CDPH), blowing the whistle to the government about Aurora's severe, dangerous, and illegal understaffing," the lawsuit says. "Less than a month later, on the day after Thanksgiving 2016, Signature and Aurora retaliated, firing plaintiff without warning because she would not silently abide the company's push for profits over the rights of patients and staff. Shortly after, CDPH substantiated and validated plaintiff's complaint about understaffing and unsafe conditions at the hospital." ■

Make Background Screens Thorough and Efficient

Healthcare organizations are improving their ability to screen job applicants for criminal backgrounds and other disqualifying factors, but it is important to screen volunteers and others just as effectively.

At the same time, be careful not to make your screening process so onerous that it drives away good applicants.

Sharp HealthCare in San Diego uses a vendor to conduct background checks after a new hire has been offered and accepted a position, says **Elmerissa Sheets**, director of workforce development and recruitment strategy. Sharp HealthCare started performing background checks about 10 years ago.

"The background check includes criminal records, and that is very important to us as a healthcare provider," Sheets says. "We do that with every single candidate and they are not fully hired — they can't start working — until that comes back. If there are issues with the report, our vice president and human resources director check into it."

More Thoroughness Needed

The health system has had to rescind offers after the background check revealed criminal convictions that the candidate did not divulge, Sheets says. Out of about 3,500 hires a year, about 40 offers are rescinded for background screening reports and similar issues.

In the past 15 years, she has seen more healthcare organizations perform background checks, prompted in part by hospitals that thought they were performing a sufficient check by looking for a criminal record in their own states.

"We feel like we're at a high risk if we don't do it, because we're a healthcare company and have to trust people with our patients," Sheets says. "One concern is people having convictions in other states, which is more difficult for us to determine on our own, so we use a vendor that can do a broader background check."

Anonymous References Can Work

Sharp HealthCare changed its policy on references four years ago, after finding that the traditional method of calling former employers for a reference was yielding poor results. Concerns over liability have companies refusing to give references on past employees, so Sharp HealthCare switched to a vendor that collects information from past employers, some of it including detailed ratings of skills, and provides it anonymously to Sharp HealthCare.

Litigation concerning hiring decisions often can be traced back to earliest stages of the process, says **Christopher M. Trebilcock**, JD,

principal with the law firm of Miller Canfield in Detroit.

"So many times when I get involved in litigation on the back end of a hiring decision, I look at the beginning of the application and onboarding process and see gaps, things that were not completely filled out," he says. "Often, corporate risk management has provided forms for going through the due diligence to make wise hiring decisions, but then you go through those forms and too often see that they are incomplete. It's more difficult to police when the applicant gives inaccurate information, but a lot of times it was just incomplete and nobody objected."

Screen the Candystripers

Some companies are moving toward online application systems that prohibit moving on to the next question without answering the current one, he notes.

"It goes to the basics. You absolutely have to insist on complete information in the application process, and then you have to verify that information," he says. "There are people who provide incomplete or inaccurate information and just hope that a busy human resources manager will gloss over it."

It also is important to screen everyone who works in the healthcare organization in any capacity, says **Mary O'Loughlin**, managing director of healthcare at HireRight, a background screening company. HireRight recently found that background screening uncovered issues in 83% of junior-level candidates, 35% of mid-level candidates, and 14% of senior-level candidates in the healthcare industry.

> "YOUR PROCESS NEEDS TO BE THOROUGH WITH SCREENING, BUT IT ALSO NEEDS TO PROMISE THAT THE CANDIDATE GETS THROUGH THE PROCESS QUICKLY AND WITHOUT MUCH HASSLE."

"Everyone thinks of screening job applicants, but you also have to screen volunteers, contingency labor, anyone who is potentially going to be in your organization in some capacity," she says. "You should be screening those people with the same level of rigor and caution as you do for your full-time employees. A lot of times volunteers or contingent labor will have similar access to patients, protected information, and drugs that your full-time employees have."

O'Loughlin notes that the turnover experience in healthcare is higher than for other industries — about 19% — and the unemployment level in healthcare typically is about half of the overall rate. That puts pressure on the employer to have an effective and efficient screening program.

"Your process needs to be thorough with screening, but it also needs to promise that the candidate gets through the process quickly and without much hassle. A candidate who has a good experience with your application and screening process may stay longer and recommend your organization to others," O'Loughlin says. "But if the experience is lengthy or overly complicated, that candidate may turn to other employment opportunities. You can't let that discourage you from doing thorough background screening, but you also have to factor the applicant experience into how you design your processes." ■

SOURCE

- **Mary O'Loughlin**, Managing Director of Healthcare, HireRight, Irvine, CA. Phone: (949) 428-5800.
- **Elmerissa Sheets**, Director of Workforce Development and Recruitment Strategy, Sharp HealthCare, San Diego. Phone: (858) 395-8616.
- **Christopher M. Trebilcock**, JD, Principal, Miller Canfield, Detroit. Phone: (313) 496-7647. Email: trebilcock@millercanfield.com.

EXECUTIVE SUMMARY

Healthcare organizations are finding ways to conduct thorough background screens and obtain references from past employers. The process should be thorough, but not unnecessarily discourage applicants.

- Anonymous references can be effective.
- Screen volunteers as much as you screen job applicants.
- Avoid losing good applicants to a burdensome screening process.

NIST Provides Guidance on HIPAA Passwords

HIPAA regulations require healthcare entities to enact procedures for creating, changing, and safeguarding passwords, but they don't specify the details or the required complexity of the passwords. The HHS Office of Civil Rights (OCR) looks to the National Institute of Standards and Technology (NIST) for guidance, so risk managers also should, one expert suggests.

Traditionally, NIST recommends passwords be complex in that they require a minimum of eight characters, a mix of upper- and lower-case characters, contain numbers, and include symbols, says **Jeannie O'Donnell**, CIA, CISA, CPC, CHC, senior consultant for advisory services with Change Healthcare in Nashville, TN.

They recommend prohibiting password reuse for a set number of times and include the minimum number of characters that must be changed. They also recommend that a temporary password be changed on its first use, and enforcing password expiration. Currently, NIST recommends not enforcing password expiration unless it is necessary, she says.

"Examples are when a password is lost or forgotten, when a phishing attack has occurred, or when a password database has been compromised," O'Donnell says. "Requiring the frequent change of passwords can lead to the user creating a pattern that can be guessed."

Updated NIST Guidelines

NIST has updated its Digital Identity Guidelines (NIST Special Publication 800-63B), which includes revisions to its advice on the creation and storage of passwords. Digital authentication helps to ensure only authorized individuals can gain access to resources and sensitive data, O'Donnell explains.

> "SECURITY IS ONLY AS GOOD AS THE USERS OF THE SYSTEM, SO PERIODIC TRAINING IS RECOMMENDED TO ENSURE USERS UNDERSTAND THEIR SECURITY OBLIGATIONS AND THE IMPORTANCE OF REPORTING SUSPECTED ACCOUNT COMPROMISES."

NIST states that "authentication provides reasonable risk-based assurances that the subject accessing the service today is the same as the one who accessed the service previously." The guidelines are not specific to the healthcare industry, O'Donnell notes, although the recommendations can be adopted by healthcare organizations to improve password security.

In the security industry, the latest recommendations on password creation include using passphrases, O'Donnell says. A passphrase is a sentence or phrase, with or without spaces, typically more than 20 characters long. The words making up the passphrases should be meaningless together to make them less susceptible to social engineering.

"Another recommendation is to block dictionary words because a common problem with complex passwords is the ease of guessing them. Hackers have tested for commonly used passwords such as Winter2017, often used as a temporary password, and Steelers2017, at the beginning of football season," she says.

No matter how strong the intention to keep systems secure, administrators may be limited by the password parameters allowed by their applications.

"I recommend a single-sign application to allow for enforcement of the desired password complexity and parameters. The single sign-on can also include multifactor authentication, a method of access control in which a user is only granted access after successfully presenting several separate pieces of evidence to an authentication mechanism," O'Donnell says.

Periodic Training Required

That evidence typically is at least two of the following categories: knowledge (something they know, such as a PIN); possession (something they have, like a token), and inherence (something they have, such as a fingerprint).

"Security is only as good as the users of the system, so periodic training is recommended to ensure users understand their security

obligations and the importance of reporting suspected account compromises," she says. "In the healthcare industry, I've seen applications with two-character passwords where the providers used their initials. I've also seen passwords that were 12 characters long with a combination of letters, numbers, and symbols where the users had no choice but to write them down, but unfortunately left them visible in an unsecure location."

In encountering resistance to strong passwords, remind users that the cost of a breach, monetarily and in reputation, will far exceed the cost of compliance, she advises. ■

SOURCE

- Jeannie O'Donnell, CIA, CISA, CPC, CHC, Senior Consultant for Advisory Services, Change Healthcare, Nashville, TN. Phone: (888) 363-3361.

Lawsuit Calls HHS 'Overly Restrictive' on Charges for Secure Access

Medical record retrieval firm Ciox Health is suing the Department of Health and Human Services (HHS) for "unlawfully ... and capriciously" restricting the fees healthcare providers and their medical record vendors can charge for gathering and disseminating HIPAA-protected health information.

The fee restrictions threaten to bankrupt medical record providers, according to the lawsuit filed in the Washington, DC, circuit court against Acting HHS Secretary Eric Hargan. The company claims that the $6.50 flat fee established by HHS regulations for electronic copies of PHI is "irrational, arbitrary, capricious, and absurd."

Ciox Health claims in the lawsuit that changes implemented by HIPAA Omnibus regulations in 2013 and modified in 2016 "threaten to bankrupt the dedicated medical-records providers who service the healthcare industry by effectively and quite deliberately mandating that they fulfill a rapidly growing percentage of requests for protected health information at a net loss."

The previous regulatory changes broadened the medical information that patients can request transmitted from any form whatsoever "to any third party, including profit-seeking commercial parties like insurers and lawyers."

But those changes also limited the fees providers can charge for answering a patient's record request.

> THE COMPANY CLAIMS THAT THE $6.50 FLAT FEE ESTABLISHED BY HHS REGULATIONS FOR ELECTRONIC COPIES OF PHI IS "IRRATIONAL, ARBITRARY, CAPRICIOUS, AND ABSURD."

That puts medical record providers in an untenable position because they must comply with requests, but are not allowed to charge enough to make that service profitable, the lawsuit says.

The process is time-consuming, Ciox Health says, and once the PHI is located, it takes significant effort to fulfill a request for paper or electronic copies of patient medical records in a manner that complies with both federal law and state privacy laws, the company says.

"Producing such information in accordance with these laws is both complex and costly," Ciox Health alleges in the complaint. "The costs required to fulfill each request for a patient's PHI include not only the supplies and technology used to produce PHI to the requesting party, but also the extensive labor costs associated with receiving, compiling, verifying, and processing such requests. In many cases, these materials are located in multiple physical and virtual locations, which requires staff to be dispatched to physically obtain or retrieve records from an array of sources."

The $6.50 flat fee is not the maximum allowed by HHS. The agency's website explains that $6.50 is established as an option for when the medical records provider does not wish to calculate the actual cost of providing the records.

HHS Guidance issued in May 2016 explains that "$6.50 is not the maximum amount that can be charged for all individual requests for a copy of PHI under the right of access." The agency adds that "charging a flat fee not to exceed $6.50 is an option available to those

entities that do not want to go through the process of calculating the actual or average costs for requests for electronic copies of PHI maintained electronically as permitted by the Privacy Rule." ■

$3.77 Million to Resolve Kickback, Medical Necessity Claims

A laboratory and the owner of a lab management services company agreed to pay a total of $3.77 million to resolve claims that they were involved with illegal kickbacks and filed claims for services that were not medically necessary.

The case sends a signal to the healthcare industry that federal prosecutors have their on eye on the lucrative urine toxicology and diagnostic testing industry, a former DOJ attorney says.

U.S. Attorney Erin Nealy Cox, JD, of the Northern District of Texas, announced recently that Primex Clinical Laboratories has agreed to pay $3.5 million to resolve allegations that it violated the False Claims Act by paying kickbacks in exchange for laboratory referrals for patient pharmacogenetic testing. In a related settlement, Mitch Edland, the chief executive officer and owner of DNA Stat, agreed to pay $270,000 to resolve similar allegations.

Primex is a licensed clinical laboratory providing clinical diagnostic testing services, including pharmacogenetic testing, and DNA Stat was a laboratory management company that employed sales representatives and licensed pharmacists. The two companies entered into a services agreement related to pharmacogenetic testing services, Cox explained.

Two whistleblowers alleged that Primex submitted claims to Medicare that were rendered false as a result of Primex and DNA Stat providing kickbacks from June 2013 through March 2016.

"The relators alleged several kickback schemes, including a scheme where the defendants created the appearance of paying physicians to provide clinical study data for a Primex-sponsored study related to pharmacogenetic testing when, in fact, the physicians were being paid for referring patients for the testing," Cox announced. "The relators also alleged a scheme where the defendants provided physicians with in-office medical technicians to do work related to the Primex-sponsored study in an effort to induce those physicians to order pharmacogenetic tests from Primex. Finally, the relators alleged that the pharmacogenetic tests were not medically necessary."

Growing Federal Focus

Prosecutors also contend that DNA Stat's agreement with Primex, as well as its agreements with its sales representatives, took into account the volume and value of referrals physicians made to Primex for pharmacogenetic tests when calculating compensation.

The case signals a federal focus on this area of medicine, says former assistant U.S. Attorney **Jason Mehta**, JD, now an attorney with the Bradley law firm in Tampa, FL.

"This settlement reflects the Department of Justice's continued focus on fraud in the urine toxicology and clinical diagnostic testing areas," Mehta says. "As more and more money is spent on clinical testing, these services will continue to be a growth area for healthcare fraud prosecutions and I expect the department's interest, as well as whistleblowers' interest, will only continue in the coming months and years."

The settlement with Primex resolves the allegations centered on providing in-office medical technicians to physicians; entering into improper sales and services agreements; and submitting claims for pharmacogenetic tests that were not medically necessary.

The whistleblowers were former sales representatives for DNA Stat. They will receive $754,000. ■

SOURCE

- **Jason Mehta**, JD, Bradley, Tampa, FL. Phone: (813) 559-5532. Email: jmehta@bradley.com.

COMING IN FUTURE MONTHS

- Career tips in risk management
- Anesthesia-related liability claims
- EHR can reveal false entry claims
- Strategies for reducing alarm fatigue

HEALTHCARE RISK MANAGEMENT™

CME/CE INSTRUCTIONS

To earn credit for this activity, please follow these instructions:
1. Read and study the activity, using the provided references for further research.

2. Log on to AHCMedia.com to take a post-test, then select "My Account" to view your available CE activities. First-time users will have to register on the site using the 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.

4. After successfully completing the test, a credit letter will be emailed to you instantly.

5. Twice yearly after the test, your browser will be automatically directed to the activity evaluation form, which must be completed to receive your credit letter.

CME/CE QUESTIONS

1. **What was one issue that Hospital Sisters Health System (HSHS) Sacred Heart Hospital in Eau Claire, WI, and St. Joseph's Hospital in Chippewa Falls, WI, addressed to improve their Leapfrog patient safety scores?**

   a. Retained surgical items
   b. Violence by behavioral health patients
   c. Use of restraints
   d. Fire safety

2. **With the short-wavelength ultraviolet (UVC) light system used at the HSHS hospitals, what was one strategy for minimizing the time required to use the device?**

   a. The device is used in only one location for each room.
   b. The device is placed in the bathroom while the housekeeper cleans the rest of the room.
   c. Housekeepers use the device only on alternate days for any particular room.
   d. The exposure time was set below the minimum recommended by the manufacturer.

3. **When Upstate Golisano Children's Hospital in Syracuse, NY, implemented red lights to indicate no-interruption zones, what type did it choose?**

   a. Lights mounted on the ceiling in a fixed location on the unit
   b. Lights mounted on the mobile carts that nurses use to administer medications
   c. Lights mounted in each patient room in a fixed location
   d. Lights worn on each nurse's identification lanyard

4. **In her lawsuit against Aurora Santa Rosa Hospital, an acute psychiatric facility in Sonoma County, CA, what does former chief nursing officer Teresa Brooke allege?**

   a. The company put profits ahead of patient and employee safety, and fired her for reporting it to state authorities.
   b. The company asked her to fabricate documents showing fewer incidents of violence than had actually occurred.
   c. She was fired for refusing to take on additional staff from a sister facility.
   d. She was fired for questioning the qualifications of the chief medical officer.

LEGAL REVIEW & COMMENTARY
EXPERT ANALYSIS OF RECENT LAWSUITS AND THEIR IMPACT ON HEALTHCARE RISK MANAGEMENT

Jury Awards $2 Million for Negligent Hand Surgery

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

***Jamie Terrence**, RN*
President and Founder, Healthcare Risk Services
Former Director of Risk Management Services (2004-2013)
California Hospital Medical Center
Los Angeles

***Morgan Lynch**, 2018 JD Candidate*
Pepperdine University School of Law
Malibu, CA

News: In 2013, a boat builder suffered a hand fracture when an unsecured kayak fell on his hand. He received surgery on his hand, including the insertion of screws. The surgeon was confident the screws were properly encased, but the patient experienced unusual pain and discomfort following the surgery. After reviewing later scans of the patient's hand, the surgeon still maintained that the surgery was successful.

The patient received a second opinion from a different surgeon, who discovered that a screw was not sufficiently encased and was contacting the patient's wrist joint, causing his pain and discomfort. That surgeon removed the screw, and the patient was forced to undergo three additional surgeries.

The patient filed suit against the hospital and the initial surgeon, claiming loss of wages, permanent disfigurement, and impairment. After several days of trial, a jury found in favor of the patient and awarded him $2 million.

THE PATIENT RECEIVED A SECOND OPINION FROM A DIFFERENT SURGEON, WHO DISCOVERED THAT A SCREW WAS NOT SUFFICIENTLY ENCASED AND WAS CONTACTING THE PATIENT'S WRIST JOINT, CAUSING HIS PAIN AND DISCOMFORT.

Background: A 49-year-old man suffered a fractured right wrist after a kayak fell on him in 2013. Several months thereafter, the patient underwent hand surgery. The surgeon recommended and performed a bone graft and inserted a compression screw into the man's scaphoid bone. However, later scans revealed that the compression screw protruded out of the bone and stuck into the patient's wrist joint.

The surgeon also failed to recognize the protrusion on follow-up scans. When the patient sought a second opinion, a different surgeon noted the error and removed the screw, but the patient required multiple surgeries to treat the damage and continued to experience pain and loss of function in his wrist.

The patient sued the physician and the hospital in 2015, alleging that the physician failed to properly insert the screw in his hand during the surgery. He further contended that as a direct result of the physician's negligence, he suffered wrist complications that required three subsequent surgeries to remedy. The patient requested damages for loss of income, permanent disfigurement, and impairment.

At trial, the plaintiff focused on the fact that he lost function in his dominant hand, the hand he used extensively for his work as a boat builder. However, the foundation of the plaintiff's case was established during discovery. During his deposition, the surgeon claimed he was certain that he had properly placed the screw, but at trial he indicated that the screw may have been flush with the bone instead of encased. This discrepancy between the deposition and trial testimony was a major focus of the plaintiff's case.

The defense contended that the physician gave the patient quality care, and therefore conformed to the applicable standard of care. The defense argued that treating a fracture is particularly difficult. Both the plaintiff and the defense called experts who chair orthopedic hand surgery departments of major medical centers. Unsurprisingly, the experts disagreed on the specifics of appropriate treatment for a hand fracture. The trial lasted four days, and the nine-member jury deliberated for two hours before rendering a verdict in favor of the plaintiff for $2 million in damages.

The plaintiff's counsel participated in several press releases, one of which included the statement that people put trust in "doctors and hospitals to treat them with the same level of planning and care they would expect for their own loved ones."

What this means to you: A major factor in this case was inconsistency in the physician's testimony. Had the physician maintained consistency between his deposition and the trial, he may have retained more credibility with the jury. This kind of inconsistency usually is the result of poor preparation before the deposition or before the trial, or both.

Relatedly, creating a reliable medical record is crucial to a defensible position in litigation, and as such, medical professionals must be educated on how to establish an accurate and consistent record. Vendors offer options for organization of the record as well as intuitive interfaces that can help minimize the inadvertent omission of material facts.

Regardless of the method used for creating and maintaining the record, hospitals should create a standard procedure for all medical professionals and staff. Moreover, if litigation occurs, a witness should review the relevant medical records prior to the deposition — and seek the advice of counsel in connection with and prior to doing so — to refresh the witness's recollection. Before trial, witnesses should prepare and be refreshed again, including review of the medical record and the deposition transcript, to ensure accuracy and consistency. Close consultation and preparation with attorneys is critical throughout litigation, but if trial is imminent, even more significant time and resources must be allocated to guarantee a thorough and successful defense.

THIS CASE ALSO PRESENTS YET ANOTHER INCENTIVE FOR AVOIDING LITIGATION: THE PREVENTION OF BAD PRESS.

This case also presents yet another incentive for avoiding litigation: the prevention of bad press. A significant nonmonetary benefit of settling cases is the mitigation of negative publicity. The plaintiff's counsel in this case implied that the physician here was remiss in his surgery, performing in a way that would disappoint one's family. Such bad publicity can be significantly damaging to a hospital and physician, to the extent that mitigating this risk should factor into a litigation analysis.

The physician's failure to recognize the protrusion of the screw in the patient's scan raises the issue of adequate care when following up with a patient. A scan is only as good as the physician's interpretation. A radiologist's review, routine in most institutions, may have helped to either confirm proper placement of the screw or to alert the surgeon to screw protrusion. Another factor the surgeon should have considered was the patient's postoperative level of pain. Was the patient's pain level appropriate for the procedure performed, compared to others who underwent the same surgery? Often, assumptions are made that a patient may have a low pain threshold, but this is an unfortunate and dangerous assumption to make. Complaints of pain that extend beyond what is anticipated warrant investigation. Exercising sufficient care during a follow-up appointment can avoid costly complications with a patient's treatment.

Bearing that in mind, physicians and other medical professionals nonetheless invariably miss things when reviewing scans. Therefore, creating a system of review procedures may be a wise business decision for hospitals. The time cost of reviewing physicians' work must be weighed against the benefit of higher diagnosis accuracy. Such a determination would require support from data gathered from physician misdiagnoses. Additionally, hospitals must consider whether instituting a review policy would step on the toes of physicians and communicate a lack of trust and respect for their professional effectiveness. Ultimately, the benefits of a review policy may outweigh any negative aspects, and should, at a minimum, be considered. ■

REFERENCE

Decided Oct. 23, 2017, in the Superior Court of Maine; Case Number CV-15-137.

Negligent Transport of Patient Leads to Paraplegia, $8.05 Million Verdict

News: In 2011, a man was driving to an airport to board a flight for his work as an aerospace configuration manager. It was still dark as he looked at the traffic around him and pulled out from an intersection. As he made a turn, the man's car was struck broadside by another car, requiring he be extracted from the vehicle. Emergency medical technicians reported "an obvious loss of lower extremity sensation and limited use of his arm." The man was taken to a hospital, where he underwent emergency cervical decompression and anterior spinal fusion surgery to repair a burst cervical fracture. The neurosurgeon installed an Atlantis Vision Elite Anterior Cervical Plating System to stabilize his spine.

Three days later, while recovering from the surgery, the nursing staff attempted to transfer the man from a chair to his bed. While he was being lifted by a Hoyer lift, the patient slipped out of the sling, back into the chair and his head collided with the rear of the chair. This collision resulted in irreversible damage to his spine. The man's wife witnessed the incident, but the nursing staff failed to include it in their charting. The man and his wife brought suit, eventually resulting in an award of $6.8 million to the patient and $1.25 million to his wife for loss of consortium.

Background: On Sept. 8, 2011, a 72-year-old configuration manager presented to a hospital for emergency cervical spinal surgery. Three days later, while recovering at the same hospital, the patient claimed he suffered various permanent injuries, including paraplegia, when his nurses were attempting to move him from a reclining chair to his bed.

According to the patient, the nurses attempted to move him from a heavy reclining chair to his bed, using a Hoyer lift with an attached sling. While he was being raised and moved with the Hoyer lift, the patient began to slide out of the sling, with his legs sliding toward the floor. The nurses allegedly reacted to this situation by pushing the Hoyer lift back toward the chair.

This pushing movement caused the sling to swing toward the back of the chair in which he had been sitting. He claimed his head then struck the back of the chair with sufficient momentum to force his head toward his chest, dislodging surgical screws that were inserted during the course of the initial surgery and causing him injury.

The patient subsequently filed suit against the hospital, alleging that it was vicariously liable for the negligence of its nurses. He claimed that the nurses breached the relevant standard of care by improperly attaching the sling to his body and causing him to strike the heavy chair. He also argued that the nurses failed to properly document the incident, which led to a delay in addressing the new injury caused by the nurses. The patient sought economic and noneconomic damages, and his spouse sought damages for loss of consortium.

At trial, the hospital contended that the surgeon who performed the surgery failed to stabilize the patient's cervical spine, causing the partial paralysis. The hospital further asserted that the nurses conformed to the relevant standard of care and that the patient's injuries were not caused by their actions. Because the nurses failed to document the incident, the defense argued that the plaintiff's narrative was unsupported by the medical record. In support of its allegations, the hospital called two expert witnesses, one legal nurse consultant, and one neurosurgeon.

The patient claimed that he suffered an anterior dislocation of C7 over T1, resulting in partial paralysis. He asserted the dislocation occurred when the cervical screws were dislodged when his head contacted the chair and were aggravated by inadequate documentation of the incident, which led to a delay in treatment. The plaintiffs selected 15 experts to support their case, the specialties of which varied from standard of care to economics. Of particular importance to the plaintiff's case was the testimony given by the patient's wife, who witnessed the incident.

After the seven-day trial, the jury deliberated for 7.5 hours before delivering a verdict in favor of the plaintiff. The jury awarded $6.8 million to the patient and $1.25 million to his wife for loss of consortium. The jury did not apportion any liability to the physician who conducted the patient's initial surgery. Based on post-trial juror interviews, the jury found the defense's experts to lack credibility.

What this means to you: This case illustrates the importance of addressing new issues and symptoms as they present themselves throughout the course of caring for a patient. Physicians and supporting staff should be educated on the value of awareness as it relates to

administering quality care. Negligence can arise quickly from a failure to diagnose based on overlooking new symptoms. There is little excuse for complacency and reckless ignorance in the medical industry. Hospitals should take it upon themselves to ensure employees have sufficiently high morale to maintain the motivation to stay aware for long periods of time. Potential options for boosting morale to improve employee awareness include ensuring employees are treated with respect, receive adequate feedback, are given goals and clear expectations, and providing hospital employee retreats.

Even assuming medical professionals experience increased morale, mistakes still happen — including in the operation of cumbersome equipment. Hoyer lifts have many moving parts, and it is imperative that professionals and staff who operate them receive sufficient training. Whenever hospitals implement new equipment, medical professionals should be trained on how to correctly and safely operate that equipment, as well as how, if at all, the operation of the new equipment differs from similar or previous equipment. For example, Hoyer lifts come with different sling attachments and can be electronic or hydraulic and the use of each varies, although the lifting sequences are similar.

The facts of this case suggest that the nurses may have attempted to swivel the patient while lifting him. It is important to note that Hoyer lifts do not swivel. The proper use of the lift requires the patient's weight to remain directly over the base legs of the apparatus at all times. To avoid accidents due to miscommunication, medical professionals should take the time to explain the lifting procedure to the patient. A potential solution for operator error-related complications is to post visual instructions or written reminders on proper operation of lifts and other equipment.

Moreover, regardless of the cause of the Hoyer lift issue, the nurses' first responsibility was to put hands on the patient. Simply moving the lift in any direction while the patient is sliding off is misguided; the patient's body must first be positioned on the sling. Protecting his head and body during the scenario described can only be accomplished by physically holding on to the patient's body until safe to release. Had the nurses done this, the outcome may have been different and injuries sustained may have been lessened or completely prevented.

On a related note, it is imperative that hospitals ensure their equipment is adequately maintained and serviced. Various organizations, such as the World Health Organization, publish best practices for the maintenance of medical equipment as well as best practices related to medical equipment generally. Procedures for documenting maintenance logs and ensuring manufacturer service schedules should be implemented and followed. This prevents or minimizes negligence liability for using unsafe equipment and keeps patients and medical professionals safe. This also can provide hospitals recourse in alleging that an injury may have been caused by a defect in the design or manufacture of a piece of equipment. All injuries occurring during the use of medical equipment, whether a product or user error, should be reported to the FDA via its Medical Device Reporting website. Reporting helps all involved, such as hospitals, patients, and manufacturing companies, prepare for problems and improve the quality of their products.

Another significant issue in this case was the fact that the nurses failed to properly document the incident, which ultimately led to a delay in treatment of the patient. More untoward events go undocumented than many people would expect; the rate of unreported events is close to 7:1. This continual problem has plagued the healthcare system for decades. A few institutions have found a way using the "just culture" method to empower staff to report events without fear of reprisal. Medical professionals should be encouraged to be proactive when facing unexpected circumstances and accidents. Patients who are particularly vulnerable, such as the elderly or those recovering from surgery, require elevated care and attention if accidents occur. Medical professionals should be reminded that dealing with problems as they arise is a better course of action than waiting for another person to discover them, or hoping those problems will remain undiscovered. The sooner an injured patient is treated, the less likely he or she will be to sue hospitals. If litigation does occur, prompt treatment serves to reduce the amount of damages.

In a similar vein, it is imperative that patients who are injured by medical professionals are treated with respect. Hospitals should be prepared for the inevitable mistake by a staff member and should communicate expectations to those staff members in such a case. Disclosure, documentation, treatment, and professionalism must be prioritized. ■

REFERENCE

Decided on Nov. 21, 2017, in Fulton County State Court; Case Number 13EV017577C.

HIPAA REGULATORY ALERT

CUTTING-EDGE INFORMATION ON PRIVACY REGULATIONS

HIPAA Allows Choice in Password Security, But Use Caution

Password security for electronic protected health information (ePHI) is a fundamental part of any HIPAA compliance program, but there is no one right way. HIPAA allows a great deal of choice in how to secure data with passwords, but one must choose carefully to ensure the information is protected from both casual snooping and sophisticated hacking.

HIPAA password management requirements are quite open-ended, only specifying that one must institute "procedures for creating, changing, and safeguarding passwords," notes **Gary Nelson**, healthcare practice leader with Schellman & Company, a security and privacy compliance assessor based in Tampa, FL.

To properly determine sufficiency for password protection, organizations should perform risk assessments for the systems or services that use or house ePHI, Nelson says. While HIPAA itself does not specify minimally defined requirements, the risk assessment could be paired with password or authentication requirements from standards such as NIST, PCI, or HITRUST to help address the HIPAA safeguard and also define what would serve as optimal for the organization.

The idea of what makes a good password is shifting, says **Kenneth K. Dort**, JD, partner with the law firm of Drinker Biddle in Chicago. Security experts used to promote the idea of a long string of random letters, numbers, and symbols, with the password changed every 60 or 90 days. Now, it is more common to use a sentence the user can memorize and take the first letter of each word as the password, perhaps throwing in one or two numbers, too.

"The reason is that through that method you actually come up with a password that is more random and harder for someone to break than if you just select a few letters and numbers that don't mean anything to you," Dort says. "A supercomputer can break any password, but most people trying to get into your system are going to take a try and move on if they can't get it quickly. The method of using a sentence gives you a more secure password, and one that the user can remember without writing it on a note taped to the desk."

Different Security Options

There are technical and non-technical options, says **John Hellickson**, managing director of strategy and governance at Kudelski Security, headquartered in Phoenix. The technical solutions range from single sign on and privileged access management to password management tools.

"I believe this really comes down to usability by the persons impacted by the requirement, which goes beyond just technology. With the goal of managing access to PHI, it is key for an organization to understand the requirements of the business and its users, in addition to the technical security requirements, and balancing that with the organization's risk appetite prior to investing in any solutions."

Many organizations have enacted strict password policies, from forcing password changes on all users between 30-90 days to enforcing specific complexity requirements that make it difficult to remember. However, Hellickson says that can ultimately increase the risk that the users will engage in practices that undermine the goal of protecting access to PHI.

"What I've seen work well is encouraging users to come up with a password scheme that meets complexity requirements where they change three or more characters to make it unique for each place they log into, allowing them to easily remember and maintain good password hygiene," Hellickson offers. "This, combined with single sign-on and a simple-to-use multifactor authentication solution, is a good way for the

security organization to relax requirements on forcing password changes on such a short schedule, such as anything less than a year."

Although more complex and costly, implementing a single sign-on solution can help reduce the burden on the end user and reduce the need to remember multiple passwords in an organization, he says. These projects usually require a lot of coordination and time to implement, Hellickson says, but the more systems and associated access that can be integrated into a single sign-on solution, the less chance the end users will fall to poor password practices.

"Knowing traditional password policies aren't working, with the more complex and rigid policies having the opposite effect on protecting those passwords, single sign-on and multi-factor technologies have come a long way and provide a better user experience while also mitigating some of the issues from relying on passwords alone," Hellickson notes.

Dual Authentication Adds Security

Two-factor authentication, also known as dual authentication, is one of the best ways to greatly enhance the access control to sensitive data, Hellickson says. With two-factor authentication, users performing a sensitive function, such as accessing PHI, enter a username and password, and then receive an authorization request on a mobile device that they tap to approve. This provides users access with minimal effort.

Two-factor authentication would be considered an alternative security measure to the HIPAA password requirement, helping accomplish the same purpose but with enhanced security, Hellickson explains. Dort also supports using two-factor authentication, saying it allows the user to use a simple password to get into the system and then a more complex one that is sent to user's phone and is valid only for a short time.

"That means that even if someone gets into your system with a user's password, they still can't access PHI unless they also have that person's phone, which is very unlikely," Dort says. "Most places require you to have your phone password-protected as well if you use it at work, so you have that additional layer of security also."

Two-factor authentication is not explicitly stated as necessary to address HIPAA safeguards, Nelson notes.

"However, organizations should definitely consider two-factor authentication for systems that contain ePHI due to the inherent risks associated with inappropriate access to data or medical records that contain ePHI," he says. "If an organization is considering the pursuit of HITRUST to address HIPAA compliance, then two-factor authentication may become necessary as a HITRUST requirement."

State University of New York Downstate Medical Center in Brooklyn is considering two-factor authentication, says **David W. Loewy**, PhD, chief information security officer with the hospital. The change would address the human tendencies that can foil a simple password system, he says.

"I can go through the hospital and out of a thousand work stations, 10% of them have the password pasted to the bottom of the keyboard," Loewy explains. "Unfortunately, the healthcare community has not taught practitioners the importance of keeping passwords secure and the value of that kind of data on the dark web. We try to impress this on them, but still, people are lazy and don't understand why this is so important." Loewy notes that the most flagrant violators of password security rules are hospital candy stripers and similar volunteers.

Constant Reminders

Healthcare organizations should create a vigorous cybersecurity awareness program, Loewy says. His hospital recently developed a program that includes a logo with a fist punching through a screen and the words "You are a target!"

"People put that on their monitors to remind them that they are targets to the bad guys and that is why we're so concerned about passwords," Loewy says. "You need to be in front of people all the time reminding them."

A robust password policy is necessary, but Loewy cautions against writing the policy and procedures as one document. It is better to maintain a policy that requires passwords but separate procedures for how to use and protect them. That way, the procedures can be updated to conform to evolving technology and trends without the need to revise the policy behind them, he says.

A common mistake by organizations is simply not assessing the true or accurate level of risk associated with systems that house ePHI, Nelson says. Based on what it defines as the risk level associated with accessing ePHI, the organization may find that it has either created insufficient password access or parameters to protect their data or, to a lesser degree, that it has implemented excessive layers of authentication and password parameters that create unnecessary costs for the organization, he says.

Whatever strategies are employed, they must be tailored to the organization's particular needs, Hellickson adds. "Moving forward with an access control program that doesn't consider the business and how end users

conduct their duties is a recipe for disaster," Hellickson warns. "The key to success is to engage the business stakeholders early, and make them part of the initiative to identify and select the set of policies, processes, and technologies to comply with this requirement." ■

SOURCES

- **Kenneth K. Dort**, JD, Partner, Drinker Biddle, Chicago. Phone: (312) 569-1458. Email: kenneth.dort@dbr.com.
- **John Hellickson**, Managing Director, Strategy & Governance, Kudelski Security, Phoenix. Phone: (623) 235-2500.
- **David W. Loewy**, PhD, Chief Information Security Officer, State University of New York Downstate Medical Center, Brooklyn, NY. Phone: (718) 613-8593. Email: david.loewy@downstate.edu.
- **Gary Nelson**, Healthcare Practice Leader, Schellman & Company, Tampa, FL. Phone: (866) 254-0000.

HIPAA Restricts Some Photography, but Not All

Photography in healthcare settings is difficult to control but could lead to HIPAA violations if not monitored. How much one should try to control people taking pictures and video can be difficult to determine.

Any photo or video that could identify the patient may be subject to HIPAA restrictions, says **Trish Markus**, JD, a partner in the Raleigh, NC, office of law firm Nelson Mullins Riley & Scarborough. This includes full-face photographs but also photographs of distinctive tattoos, birthmarks, and other identifying features. Those all constitute PHI, she says, and therefore must be used and disclosed only for permitted purposes.

"There are legitimate reasons for healthcare providers to take pictures of patients, including to photograph rashes for inclusion in the patient's medical record, to submit before-and-after photos of plastic surgery patients to a specialty board as part of a physician's board certification process, and for use within the facility in educating students or clinicians," Markus explains. "Providers even may use patient-identifying images for research studies, if patients agree to this use of their PHI."

Additionally, before using photos or video of a patient for a healthcare provider's marketing or fundraising purposes, the provider must obtain the patient's written authorization outlining the manner and extent to which the images may be used, Markus adds.

Photographs that are used for treatment, payment, or healthcare operations purposes do not require patients' written authorization, Markus says. However, obtaining written consent still can be a good idea, says **Jennifer Romig**, JD, an associate with the law firm of Ropes & Gray in Chicago.

"I advise explaining in very clear terms the purpose of the photography and how it will be used, including who will see it and how it will be stored. That's best practice even though it is not strictly required for HIPAA compliance," Romig says. "Any use of patient photos for something other than the patient's care, like putting photos on your website, absolutely requires consent from the patient. You also have to make clear to them that they are free to say no."

To limit the disclosure of such images outside the organization, providers should consider permitting photographs for legitimate clinical or operational use to be taken only using facility-owned or facility-approved equipment, not clinicians' individual cellphones. "Providers should adopt a policy clarifying that any authorized photographs or videos are the sole property of the facility," Markus says. "The policy also should prohibit distribution of photographs or other images involving patients to any person outside the facility without written authorization from the patient for a permissible use."

Staff should be trained on the organization's policy regarding photography and the consequences of violating it. Staff also should be trained to require individuals observed in violation of the policy to stop the photographic or video recording activity. Controlling photography by employees is one thing, but how much should healthcare organizations control what patients, family, and visitors do with photography? Given the ubiquity of cellphones and their enhanced photography and video recording capabilities, it's important for healthcare providers to consider implementing a policy that addresses whether and how patients, their family members, and their friends may use photography and video while on the premises of the provider, Markus says. Most facilities find that policing non-staff use of photography is too difficult and don't implement detailed restrictions, Romig says.

"Personal photography by patients, family, and visitors is very difficult to control. If people are taking pictures of relatives or people they know, hospitals generally are getting in the way of that," Romig says. "But there are facilities in which if staff see people

taking pictures of an unconscious person, or other patients they may not know, the staff will intervene and ask them to stop. Practically speaking, that is a difficult thing to catch because people have their phone out all the time and sometimes you don't even know when they're taking pictures."

However, some restrictions may be necessary. Markus provides these examples to demonstrate different reasons for proactively addressing patients' use of cameras in the healthcare setting:

• In 2008, at the University of California, Los Angeles' Resnick Neuropsychiatric Hospital (Resnick Hospital), a patient violated the privacy of other patients by taking photographs during a group therapy session and posting the photos to a social networking website. The patient who posted the photos claimed that other patients consented to the photographs, but hospital administrators rejected this assertion and expressed concern that, due to the nature of the group session, the patients involved may not have been fully competent to give their consent.

• Patients sometimes take pictures of their loved ones in the hospital and share those images on social media sites. However, if the patient is not in a private room and the patient's roommate is in the picture, or if the picture of the patient includes other patients participating in a physical therapy session, the taking and sharing of such photos without the other patients' consent creates privacy headaches for providers.

• Family members sometimes wish to document physical conditions of healthcare facilities or the quality of the care their loved ones are receiving in a facility. They may take photographs of the patient's room or other parts of the building. In some cases, family members set up hidden cameras to videotape the patient's care or surreptitiously record discussions with clinicians or staff. These family members then use the photos or video recordings as leverage in litigation over patient care concerns. HIPAA clearly does not permit healthcare providers to use and disclose photos that contain PHI for purposes such as a staff member's curiosity or prurient interest, Markus says. Unfortunately, this kind of privacy violation happens. Markus offers these examples:

• In a particularly egregious case, doctors and nurses at the University of Pittsburgh Medical Center Bedford used their personal cellphones to photograph and videotape the genitals of a man under anesthesia who was undergoing surgery to remove a foreign body that had caused a genital injury. These staffers shared the pictures with other personnel at the hospital who were not involved in the patient's care. This occurred despite the hospital's policy prohibiting photography that is not intended for educational use or for the benefit of the patient.

• An EMT student who photographed an emergency room patient suffering from a severe facial gunshot wound with her personal cellphone; the student then shared that photo with friends and colleagues in her training class, ostensibly in part for educational purposes. The facility determined that emergency room clinicians and staff present while the student was taking photos, including one of the student's instructors, should have advised the student to refrain from taking the photos, and the facility instituted disciplinary action against those present and reviewed its arrangement with the institution providing the instruction.

Additionally, some obstetric practices are taking down their "baby walls," bulletin boards covered with pictures of smiling babies, in response to concerns that posting such pictures violates HIPAA unless the patient (or, in an infant's case, the patient's parent or guardian) has signed a written HIPAA authorization permitting the posting. Although the article noted that some physicians believe that babies' faces are anonymous, fertility physicians acknowledge that posting photos of babies with their birth mothers could violate the privacy of the adoptive mothers.

Healthcare facility policies limiting photography and video recording vary widely, Markus says, but they should address both staff and patient/family member activities. Healthcare providers should conspicuously post signs that clearly state the nature and extent of the limitation on camera and video use within the facility so that volunteers, visitors, patients, employees, and practitioners all understand what is permitted.

Following the group therapy incident, Markus says, Resnick Hospital instated a complete ban on the use of any cellphones or laptops within the facility, regardless of whether such phones or laptops included a camera. The hospital took this measure in lieu of requiring staff to check whether cellphones or laptops contained cameras.

"Ten years later, the idea of completely banning the use of cellphones or laptops in any healthcare provider environment seems unworkable," Markus says. "However, it is realistic and appropriate to set some limits by reminding patients and visitors to respect other patients' and visitors' privacy by refraining from photographing or videotaping anyone other than the patient." ■

SOURCE

- **Jennifer Romig**, JD, Associate, Ropes & Gray, Chicago. Phone: (312) 845-1234. Email: jennifer.romig@ropesgray.com.