FOR MORE THAN 30 YEARS

HOSPITAL ACCESS MANAGEMENT™

ADMITTING + REIMBURSEMENT + REGULATIONS + PATIENT FINANCIAL SERVICES + COMMUNICATIONS
GUEST RELATIONS + BILLING & COLLECTIONS + BED CONTROL + DISCHARGE PLANNING

JUNE 2017 Vol. 36, No. 6; p. 61-72

INSIDE

Enclosed in this issue:

HIPPA Regulatory Alert: Do you really know HIPPA?; More to HIPPA than high-tech security

Anxiety at All-time High in Registration Areas

Registrars often bear the brunt of patients' frustration

A man entered a hospital outpatient center by shooting down the door, then headed to the cardiac ICU.

"He committed suicide when the SWAT team arrived, but had held several nurses hostage for a few minutes before the situation was handled by police," says **Sara Smiley**, who was the hospital's patient access director at the time.

Around the same period, a patient set himself on fire at the ED registration desk.

"Patient access staff were obviously affected by these incidents," Smiley recalls.

Since the hospital provided both adult and pediatric psychiatric services, many staff were certified to provide Critical Incident Stress Management training.

"This was vital after the gun violence incident," Smiley says.

"THE HARDEST CHALLENGE FOR PATIENT ACCESS IS TRYING TO BALANCE PROVIDING SUPERIOR CUSTOMER SERVICE WITH ENSURING SAFETY."—SARA SMILEY, EXPERIAN HEALTH

Understandably, patient access employees were worried about their safety. Some asked for additional protections at registration areas, such as bulletproof glass.

"Many changes were put into place immediately," Smiley remembers. "Panic" buttons were added to phones, so registrars could alert security of a problem within seconds.

"The hardest challenge for patient access is trying to balance providing superior customer service with ensuring safety," says Smiley, currently a process improvement consultant for Experian Health.

Many hospitals have decentralized registration, which means there are many entrances — all open to the public.

"This was the case with our facility. We had many public entry points, and not all of them were staffed with security

HOSPITAL ACCESS MANAGEMENT

Hospital Access Management™,
ISSN 1079-0365, is published monthly by
AHC Media, a Relias Learning company
111 Corning Road, Suite 250
Cary, NC 27518
Periodicals Postage Paid at Atlanta, GA 30304 and at additional mailing offices.

POSTMASTER: Send address changes to:
AHC Media
P.O. Box 74008694
Chicago, IL 60674-8694

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

SUBSCRIPTION PRICES:
Print: 1 year (12 issues): $429. Add $19.99 for shipping & handling.
Online only: 1 year (Single user): $379
Outside USA, add $30 per year, total prepaid in U.S. 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.

Back issues: $80. Missing issues will be fulfilled by customer service free of charge when contacted within one month of the missing issue's date.
GST Registration Number: R128870672.

AUTHOR: Stacey Kusterbeck
EDITOR: Jonathan Springston
EDITOR: Jill Drachenberg
EXECUTIVE EDITOR: Leslie Coplin
AHC MEDIA EDITORIAL GROUP MANAGER: Terrey L. Hatcher

AHC Media
A RELIAS LEARNING COMPANY

guards," Smiley says, noting the hospital closed several entrances after the violent incidents. "All patients and visitors now enter through one of a few doors, all of which have security staff."

During her frequent site visits, Smiley often is surprised at the lack of security in place.

"It's kind of surprising how many hospitals just point us in the right direction, and that's it," she says. "There is a huge variety in the levels of security hospitals provide. There doesn't seem to be a standard."

Registrars Need Tools

Violence in hospitals clearly is increasing nationwide.

"Registration areas are no exception. These front-line personnel often get the brunt of a patient's, family's, or friend's frustration," says **Richard D. Roebuck Jr.**, BAAS, CHPA, MPO, captain of police for the Dallas County Hospital District Police Department, based at Parkland Health & Hospital System.

Roebuck says threats of violence and physical assaults are a concern that demand "vigilance, training, and sensitivity. Registrars are in a unique position to encounter these situations." Already-anxious ED patients lacking proper patient identification needed for registration sometimes take out their frustration on the person in front of them.

"Often the customer lashes out in an attempt to move the process faster," Roebuck says.

The registrar's three-fold challenge is to stay calm while providing excellent service, always with their own safety top of mind.

"It is a good idea to train all front-line employees on how to remove themselves from a volatile situation and not allow it to escalate to threats of violence or actual violence," Roebuck says. *(See related story on de-escalation training on the next page.)*

Roebuck says de-escalation training "is always a good idea. It puts a few tools in the registrar's tool box on how to handle unruly customers, reducing the potential for violence or assaults."

Reach Out to Hospital Experts

Mary Lee DeCoster, a Phoenix-based revenue cycle consultant, offers these suggestions for patient access leaders:

• Reach out to other departments to provide safety awareness training at regularly scheduled staff meetings.

Organizational development, education, security, social services,

EXECUTIVE SUMMARY

With violent incidents on the rise in the hospital setting, patient access departments are taking steps to protect registration staff, such as providing de-escalation training. Other approaches include:

- reducing the number of public entrances;
- adding "panic" buttons to phones to allow patient access to alert security;
- creating role-playing exercises to defuse common tense situations.

pastoral care, and compliance are good contacts.

"Training topics can be modified to fit the agenda and available time," DeCoster says.

Some examples include safety awareness, recognizing when a patient is agitated, how to defuse a tense situation, hospital policies involving active shooters, and diversity training.

• Allow time and space for an individual employee to decompress after a difficult patient encounter.

Registrars can spend a few minutes in a nearby conference room, break room, a leader's office, or a nearby restroom, for instance.

• Encourage co-workers to be alert for signs of potential conflict.

"Co-workers can move in to partner with the affected registrar, and function as a third party to defuse rising tensions," DeCoster suggests.

A colleague can interrupt the registration interview in several ways, based on personal observations of the ongoing or escalating conflict. Some examples: "Hello, my name is Mary, may I offer assistance?" "It sounds like I might be able to help, if you will allow me to do so?" "Would you like something to drink? I can provide you with some water." "I work with Mary, and believe I can help resolve this issue."

"The words used should reflect respect for the coworker, while inviting the customer to turn their attention to them for additional support," DeCoster says. ■

SOURCES

- **Mary Lee DeCoster**, Revenue Cycle Consultant, Phoenix. Phone: (602) 689-2026. Email: mldecoster@cox.net.
- **Sara Smiley**, Strategic Services Consultant, Experian Health. Email: sara.smiley@experianhealth.com.

Tips to Defuse Tense Situations

After several violent incidents occurred, registration staff at a behavioral health facility received de-escalation training. The focus was how to resolve conflicts that arise frequently in patient access areas.

"We wanted them to be able to avoid that initial escalation in the first place," says **Sara Smiley**, who was the patient access director at the time. "If the issue was something they could resolve on their own, we empowered them to do that."

If the registrars feel unable to resolve a concern, they must know the appropriate person to contact. For instance, registrars might contact the charge nurse if a patient is upset about a prescription, or involve the office manager for complaints about scheduling.

Smiley made a point of encouraging her patient access staff to be confident in a decision to call security or police. Sometimes, it can be a tough call for registrars to make. Some worry it will become a "he said/she said" situation, with possible repercussions from leadership.

To head off such concerns, Smiley says, "we reiterated that verbal abuse or violence of any kind would not be tolerated — and that it would never be incorrect to call for help."

As patient access leaders, Smiley says, "We should trust their judgment. We should have their backs." Here are three role-playing scenarios the department used during de-escalation training:

1. A patient (or parents of a patient) wants to see a nurse or physician, but they don't have an appointment.

An effective response: "I understand that you don't have an appointment but your situation is urgent, and that you need to be seen. I'll be back with you as soon as I can."

2. A patient is upset because a physician is running behind schedule, and their wait is longer than expected.

"My appointment was at 3:00, and it's now 4:00. What am I still doing here?" The registrar might be tempted to tell the angry patient, "It's not our fault! The lab is short-staffed," or "There's nothing I can do." Such responses are a bad choice of words.

Instead, Smiley suggests saying: "I understand you have been waiting at least an hour. I know how frustrating this can be. I will check with the nurse to find out the best estimate we can give you."

3. A patient is given a prescription, then finds out from the pharmacy that their insurance won't cover it.

This often happens because the patient's coverage changes from one Medicaid HMO to another with a different formulary.

The patient receives a refill, but no one realizes the new insurance won't cover the medication.

In this case, Smiley suggests saying: "I'm sorry to hear your insurance doesn't cover the prescription you've been taking for several months. We will try to get you moved to a different prescription that is covered by the new plan. If doctor says you cannot change medications, we will help you explain that to the new Medicaid plan." ■

Avoid Disastrous Results of Overly Aggressive Collecting

Patients will remember a negative experience

One of the first "touch points" a patient experiences is at registration, during which money often is collected upfront.

"A negative experience is what they'll remember," warns **Holly Lang**, a New York-based contractor specializing in healthcare financing, public policy analysis, and nonprofit hospital strategy.

"There are several issues with overzealous collections," Lang says. "Point-of-service collections is particularly tricky as hospitals increasingly look to get paid at the time of care."

Not in Compliance

Some hospitals keep patient credit card information on file and charge accordingly, even without the explicit permission of the patient at that time.

"Often buried within the paperwork the patient initially signed, he or she likely agreed for the hospital to maintain this information without realizing how it could be used later," Lang explains, noting this practice can backfire quickly. "It can create an incredible burden for the patient, who now has to deal with a large credit card bill on top of whatever medical issue brought them to the hospital initially."

Recent regulations have put into place certain timelines to which revenue departments must adhere, especially regarding lower-income patients at nonprofit hospitals.

"Unfortunately, we still see many hospitals not in compliance," Lang says.

For example, it is not uncommon for hospital registrars or patient access staff to ask a patient to provide a deposit on their care, or to settle a previous debt, before they're allowed to be seen.

"Even though hospitals are not allowed to do this in emergent or medically necessary situations, some still do," Lang says. She recommends a "softer touch" for upfront collections: "Offer additional options for the patient, such as a zero-interest payment plan." *(See related stories in this issue on how to avoid collection complaints, and how an investigation pinpointed the need for additional training.)*

Roger Stone, system manager for admission services, patient registration, and central access at CoxHealth in Springfield, MO, says the key is to make patients aware of their financial obligations before they arrive for services.

"This is most certainly a team effort that our pre-registration teams and all other staff are heavily involved in," he says. "That said, in the past few years, point-of-service collections initiatives have changed tremendously for many healthcare organizations."

Patient access must help patients understand their financial obligations, Stone says.

"It is best to try to take any surprises out of this process for the patient. Have the financial discussion over the phone during pre-registration, if possible," he offers.

Driver of Satisfaction

Tanya Powell, CHAM, patient access director for Ochsner Health System North Shore Region in Slidell, LA, received complaints about ED collections some time ago.

"Staff were sometimes showing an open display of aggravation when they were unable to collect," she recalls.

Patient access managers stepped in immediately to counsel staff that pressure to collect could be perceived as harassment — or worse, an EMTALA violation. Registrars were told that statements such as "Can't you pay something? It is only $50," were not appropriate.

"Our team was re-educated that it

EXECUTIVE SUMMARY

Overzealous upfront collections cause multiple problems for patient access, including dissatisfied patients and noncompliance with regulations.

- Offer additional options for the patient, such as zero-interest payment plans.
- Don't rush the conversation.
- Give price estimates at the same time pre-service collection calls are made.
- Ensure registrars are comfortable responding to patients' questions.

is primarily our obligation to inform the patient of financial responsibilities," Powell says. "With increased rounding and coaching, we do not experience this as much."

If the patient says he or she is unable to pay, registrars offer many options. Sometimes, they get creative in finding ways to assist the patient.

"There is an art to financial counseling," Powell adds.

Kaylyn Lambert, system director for patient experience at CoxHealth, says point-of-service collections can become a problem if not handled correctly.

"Many systems use this in a competitive format amongst their employees to drive collection dollars," she explains.

Sometimes, competition becomes too fierce, getting in the way of patient satisfaction. Lambert says the two goals actually are intertwined.

"Point-of-service collection should be utilized more as a resource for patients," she notes.

Engaging in a quality collection conversation can prevent the patient from receiving an unexpected bill. It alleviates the common worry: "How much will I owe?" However, being too aggressive leaves patients with a lasting negative impression.

"Patients could leave with the idea that the hospital only cares about one thing: money," Lambert says, adding that overzealous collectors should be coached on customer service techniques. "This behavior causes social media discussions, as well as attorney-seeking, if a patient feels that financial obligations were pushed before their health concerns were taken care of." ■

SOURCES

- **Kaylyn Lambert**, System Director, Patient Experience, CoxHealth, Springfield, MO. Phone: (417) 269-4103. Email: Kaylyn.Lambert@coxhealth.com.
- **Holly Lang**, Phone: (404) 512-8808. Email: hollylang@gmail.com.
- **Tanya Powell**, CHAM, Patient Access Director-North Shore Region, Ochsner Health System, Slidell, LA. Phone: (985) 646-5132. Email: tpowell@ochsner.org.
- **Roger Stone**, System Manager, Admission Services/Patient Registration/Central Access, CoxHealth, Springfield, MO. Email: roger.stone@coxhealth.com.

Three Ways to Avoid Most Collection Complaints

When collecting from patients, a rushed conversation from an ill-informed registrar can turn into a conflict quickly

Stacy Hutchison-Neale, CHAA, CRCR, supervisor of the hospital pre-authorization department at Wilmington, DE-based Nemours Alfred. I. DuPont Hospital for Children, says the key to avoiding complaints "is all about the approach and the tone that you take with the family."

• **Explain all options to the families thoroughly.** Patients can choose to pay by phone prior to services, pay at the time of service, or create a payment plan.

• **Don't rush the conversation.** "Our team will spend as much time as necessary with the families to make them aware of what their responsibilities for the services are," Hutchison-Neale says.

• **Give price estimates at the same time pre-service collection calls are made.** This way, says Hutchison-Neale, "the family is never blindsided."

However, registrars must be confident in the numbers they're providing. "The family wants to be sure you know what you are talking about when it comes to their benefits," Hutchison-Neale says.

Patient access staff sometimes field collection calls when the insurance verifier is out.

"We prepare prior to making any calls," she adds. "We want to be sure we can answer questions without having the family doubt our knowledge of the situation." ■

SOURCE

- **Stacy Hutchison-Neale**, CHAA, CRCR, Supervisor, Hospital Pre-Authorization Department, Nemours Alfred. I. DuPont Hospital for Children, Wilmington, DE. Phone: (302) 651-5184. Fax: (302) 651-4224. Email: Stacy.HutchisonNeale@nemours.org.

Surprising Reason for Collection Complaints

Registrars uncomfortable talking about benefits

There are certain complaints that likely are familiar to patient access staff. "The registrar was very friendly — until I asked how they came up with the amount I owed." "The registrar's tone of voice changed after I asked if she was really sure about my benefits."

Shelita Russ, CHAM, director of patient access services at Louisiana-based Ochsner Medical Center - Kenner, Ochsner Health Center - River Parishes, and St. Charles Parish Hospital, recently fielded a few similar complaints. Each time, the patient stated that the registrar had spoken rudely during a collection conversation.

Russ set out to conduct a thorough investigation by speaking with each patient. She learned that most already knew they owed something, so the fact someone asked for money wasn't the issue. Russ discovered a common thread to the complaints: The problem started when the patients questioned the amount the registrar quoted.

"I found that even some of the most experienced registrars sometimes resorted to a more assertive tone when being challenged by a patient while discussing liability amounts," Russ reports.

Patients said the registrar's body language and tone of voice changed.

"The registrar was no longer participating in an open and inviting conversation," Russ says.

When Russ observed staff from the lobby, she saw that the patients were correct: "I observed this 'change' with multiple staff." Russ spoke with her team and learned that they were very comfortable talking about the information that the insurance verifier had noted. Their discomfort stemmed from questions about the patient's coverage that was not included in the benefits summary section.

"They became uneasy. It was clear that the patient had taken them out of their comfort zone and their overall demeanor changed," Russ notes.

Better Responses Needed

It was apparent that more detailed training was needed to equip registrars to fully discuss patient liabilities.

> THE PROBLEM STARTED WHEN THE PATIENTS QUESTIONED THE AMOUNT THE REGISTRAR QUOTED.

"I also realized that there would be times in which the employee would not have the answer to the patient's questions," Russ says. Registrars needed to find a better way to respond in these instances.

Staff were asked to role play using scenarios that came up with different types of insurance issues.

"It was interesting to have the team create their very own scenarios," Russ says.

Some examples included:

• A patient had a high-deductible plan and a large liability amount, but English was not the primary language.

"The staff had the challenge of communicating the patient liability amount through the language line," Russ says.

• A patient had coverage that was terminated mid-month because of a job change, but the patient was adamant that he had coverage until the end of the month.

• A walk-in patient during lunch had a limited out-of-state policy that the staff had to call to verify.

"Additionally, this patient continued to use her cellphone during the registration conversation," Russ notes.

Some suggested scripting:

• "I can certainly look into that for you."

• "That is a really good question. Unfortunately, my notes do not include a full list of your benefits. However, I can contact the insurance company to get clarification if you would like."

Russ says these tools made all the difference: "Scripting, additional training, and knowing that they could politely excuse themselves and pull in a senior coworker to assist." ■

SOURCE

- **Shelita Russ**, CHAM, Director, Patient Access Services, Ochsner Medical Center - Kenner/Ochsner Health Center - River Parishes/St. Charles Parish Hospital, Louisiana. Phone: (504) 894-2912. Email: sruss@ochsner.org.

Inaccurate Provider Information an Often-overlooked Problem

'One of the fundamental challenges' for patient access

Patient access representatives don't really know if they're relying on accurate data to refer or schedule patients. This means some patients are matched with the wrong providers — a big dissatisfier for all concerned.

"This is one of the fundamental challenges patient access departments face across the industry," says **Travis Moore**, senior vice president of market solutions at Kyruus, a Boston-based provider of patient access solutions.

Patient access staff often end up validating information manually as they try to refer or schedule patients.

"They make decisions based on the data they have in front of them, spread across multiple databases, in thick binders, or on Post-its, and update information where they find discrepancies," Moore explains.

This inefficient process causes misdirected referrals.

"Patient-provider mismatches can lead to an increase in patient leakage out of the health system, not to mention a poor patient experience," Moore says.

However, patient access representatives are limited in what they can do. The true "owners" of provider information are elsewhere — medical staff offices, managed care offices, practice management systems, and providers.

"If the necessary provider information can be verified by these sources before it gets into the hands of patient access representatives, it increases the likelihood of appropriate patient-provider matches at the point of scheduling, and ultimately improves the patient's experience," Moore says.

Patient access call centers typically don't have clinically trained staff booking appointments. When patients ask to see someone who treats a certain condition, the best provider match often isn't apparent based on available data.

"For example, if someone is seeking help for knee pain, is the health system's top orthopedic surgeon the best provider for that patient, or is a practice's nurse practitioner the best choice as the first step toward diagnosis and treatment?" Moore asks.

It might even be that another type of provider is a better fit, such as a sports medicine expert.

"That's not easily determined due to the limited data available to patient access representatives," Moore notes.

Sometimes, patients wait weeks or months for an appointment, only to later find that the provider wasn't the best match. Both the patient and provider are unhappy.

"This can lead to friction or distrust between provider organizations and patient access centers," Moore observes.

Accurate Data Ensured

Andrew Ray, director of professional revenue cycle at Stanford (CA) Children's Health, sees three main sources for data inaccuracy issues:

1. Referral data related to the patient's condition;
2. Referral data related to the services, physician, or location where the patient is expected to be seen;
3. Patient demographic and insurance information that drives the referral, scheduling, and authorization workflows used to verify insurance coverage.

"We have rolled out an enterprise-wide approach by building referral and scheduling templates, in close coordination with the physician and clinic leadership, to improve this," Ray reports.

When processing referrals, scheduling, and authorizations, patient access staff is led through comprehensive questionnaires.

"This ensures we have complete and accurate data from the referring provider, the patient, and the insurance to complete this process," Ray says. Diagnosis codes are used to steer a patient to the correct physician or location.

EXECUTIVE SUMMARY

Outdated, inaccurate information causes patients to be matched with the wrong provider, a dissatisfier for patients and providers. Revenue cycle leaders can address this by:

- coordinating with clinical leaders to create referral and scheduling templates;
- using diagnosis codes to steer a patient to the correct physician or location;
- factoring in patient location preference.

"We also have expanded our geographic footprint significantly over the past five years, throughout the Bay Area," Ray notes.

The process weighs patient location preference, when there are two or more options, along with availability and physician preference.

"This enhances the experience for our patients and our referring providers," Ray says. ■

SOURCE

- **Andrew Ray**, Director, Professional Revenue Cycle, Stanford (CA) Children's Health. Phone: (650) 723-9810. Email: aray@stanfordchildrens.org.

Don't Ignore Future Patient Access Leaders

Encourage employees to share ideas

When **Aimee Egesdal**, manager of patient access at Genesis Health System in Davenport, IA, meets with another department, she often brings one of her best employees along. This gives the employee a chance to meet new people.

"Since they do the work daily, they tend to have great ideas to share, especially when we are meeting on a process improvement idea," Egesdal says.

Recently, Egesdal attended a meeting with a physician office with which patient access was experiencing some difficulties. She brought a patient access staff member along.

"She appreciated being included, as she could speak firsthand on the concerns and offer suggestions for improvement," Egesdal recalls. The office manager liked the idea, and brought her own staff members into the discussion. The patient access employee enjoyed being part of the process.

"It's important for staff to see how to have those 'difficult' conversations in a positive and constructive manner," Egesdal says.

When new projects are under implementation in patient access areas, Egesdal asks employees with leadership potential to explain the changes to their colleagues.

"Recently, at one of our critical access hospitals, my lead registrar participated in a week-long 'Lean' event on how to improve the infusion process," Egesdal says, noting the lead registrar then trained her co-workers in how the new process would affect registration. "Staff like to listen to their co-workers. They tend to be able to sell the idea or change better."

David Kelly, director of revenue cycle management at Mary Rutan Hospital in Bellefontaine, OH, likes to give employees "ownership" when an issue comes up in the department. Recently, there was a scheduling dispute.

"Rather than push out a top-down solution, our patient access supervisor brought the shift employees together and asked them to resolve the situation themselves," Kelly says.

Another recent example involved a training guide for the hospital's communications system, for which patient access is responsible.

"Rather than just put together a training guide that we thought would work, we asked some of our key employees to do the initial draft," Kelly says. ■

SOURCES

- **Aimee Egesdal**, Manager, Patient Access, Genesis Health System, Davenport, IA. Phone: (563) 421-2235. Fax: (563) 421-3608. Email: EgesdalA@genesishealth.com.
- **David Kelly**, Director, Revenue Cycle Management, Mary Rutan Hospital, Bellefontaine, OH. Phone: (937) 651-6338. Email: David.Kelly@maryrutan.org.

EXECUTIVE SUMMARY

Patient access leaders can informally encourage future leaders by bringing employees to meetings with other departments and asking them to give presentations. Employees can:

- offer suggestions to resolve difficulties with a physician office;
- train colleagues on how new clinical processes affect registration;
- resolve scheduling disputes;
- create the initial draft of training manuals.

Get Future Leader to Go Outside Comfort Zone

It's important to "stretch someone out of his or her comfort zone" if one believes an employee demonstrates leadership potential, according to **Amanda Taylor**, MBA, CHAM. She recommends these techniques:

• Email articles or videos that touch on a specific leadership point, and ask what the employee thinks.

"This encourages the employee to reflect on the topic," says Taylor, director of patient access and medical records at United Regional Health Care System in Wichita Falls, TX. For good conversation starters, look for short articles on LinkedIn on communication, motivating, and inspiring your team, how to achieve goals, and improving patient experience scores.

• **Ask the employee to present at a department meeting.**

"Most of us have some level of anxiety with public speaking. The best way to work through that is with practice," Taylor says. Good topics to assign: Medicare as Secondary Payer, scripting for point-of-service collections, or information on a fundraiser that the department is working on.

• **Invest in training.**

"If you have a department budget available for external training, consider sending some of your up-and-coming leaders," Taylor says.

• **Pair the employee with someone he or she can go to for feedback, other than a direct supervisor.**

This may be a current leader in the department, or a person from another department that patient access works with closely. "Or make your future leader a mentor to a new employee within the department," Taylor suggests.

• **Encourage employees to take any opportunity to lead.**

This includes volunteering for fundraising activities for schools or churches. "Anything that gives them an opportunity to put their leadership skills into practice will prepare them for future opportunities," Taylor says. ■

SOURCE

- **Amanda Taylor**, MBA, CHAM, Director, Patient Access and Medical Records, United Regional Healthcare System, Wichita Falls, TX. Phone: (940) 764-6105. Fax: (940) 764-6093. Email: amtaylor@unitedregional.org.

Patients' Transgender Identity Resulting in Denied Claims

This is an 'evolving area' in registration

If gender isn't indicated correctly at registration, it can result in inappropriate claims denials, hours of phone calls trying to correct the problem, and incredible frustration on the part of the patient. Yet, most patient access departments have no way to address these problems involving transgender patients.

"Gender identity is an evolving area that affects registration, intake, and subsequent care," says **Kathleen Shostek**, RN, ARM, CPHRM, vice president in the healthcare risk management and patient safety division of Sedgwick, a third-party administrator for professional liability claims.

Most registration systems give only two choices: male or female.

"But we have transgender individuals and those who do not identify with one or the other," Shostek explains. This can cause claim denials, as with a patient whose birth gender is male and requires a prostate-specific antigen test, but now identifies as female.

EXECUTIVE SUMMARY

Transgender patients' gender often is indicated incorrectly at registration. This results in inappropriate claims denials for patient access and difficulty obtaining needed care. Patient access leaders can:

- instruct registrars to ask patients how they want their gender listed, without making assumptions;
- work with vendors to change systems to accept multiple gender codes;
- ensure clinical systems allow for gender identification other than the assigned sex at birth.

Melissa A. Salyer, CRCR, director of patient access at Chesapeake (VA) Regional Healthcare, says that in her 15 years of experience, "registering and billing procedures for transgender patients has always been a challenge and concern in the hospital community."

Salyer has personal knowledge of the challenges faced by the transgender community. Her son has experienced barriers to care access when he has sought care for health concerns that do not align with his identified sex.

"He has spent countless hours on the phone with billing offices, clinical teams, and his insurance carrier to ensure payment to those providing his healthcare," Salyer says.

As a patient access director, Salyer has seen similar situations arise many times. Recently, she asked other providers how they are registering this patient population in several national forums, but received only one response.

"Though the clinical systems have sections to alert team members of gender identification other than the assigned sex at birth, the financial systems are not quite so savvy," Salyer notes. Here are some challenges:

• Registration systems that only allow "male" or "female" as a selection.

The problem: If a patient identifies as male and legally is male but coming in for a hysterectomy, most systems would legally register the patient as male.

• Post-service, an account edit would fail at coding for gender/procedure matching.

This means the coding team needs to change the sex to female to get the account coded. Once coded, the billing team would need to be alerted, as they may receive a "medically unlikely" edit, and would need to change the sex to allow for the claim to bill.

• If the insurance lists the gender as male, there is still a chance of failure at the payer level.

"Edits may show that the procedure is not appropriate for the assigned gender," Salyer explains.

System integration is another obstacle.

> "THE TRANSGENDER COMMUNITY HESITATES IN REACHING OUT FOR MUCH-NEEDED CARE SIMPLY BECAUSE THEY ARE FRUSTRATED WITH CONTINUALLY EXPLAINING THEMSELVES TO THE INDIVIDUALS INVOLVED IN THEIR CARE."

"Many providers these days have connected systems to physician's offices and other data-sharing networks for regional medical record information sharing," Salyer notes.

If any one of those systems is not prepared to handle gender identity issues, it could change the patient's appropriately recorded gender in other systems.

"The transgender community hesitates in reaching out for much-needed care simply because they are frustrated with continually explaining themselves to the individuals involved in their care, financial team members included," Salyer says.

To address this issue, she recommends the following actions for patient access:

• Review the regulatory guidance associated with Section 1557 of the Affordable Care Act, and ensure compliance with the recommendations from the Office of Civil Rights (OCR).[1]

"Healthcare systems need to not only ensure adherence to the regulation, but provide seamless and compassionate access to care for this patient population," Salyer says.

The language of the OCR document prohibits payers from discriminating against transgender individuals if they seek care for health issues that are provided to them appropriately, regardless of the individual's sex assigned at birth, gender identity, or recorded gender.

For example, a covered entity would not be able to deny, based on the individual's identification as a male, treatment of ovarian cancer if the treatment is medically indicated.

• Train registrars to address the patient in their identified gender, without making assumptions.

For instance, a registrar might ask: "How shall I list your gender in our system?" Most don't ask the question at all. Instead, they use documentation and visual observation to determine gender.

"Asking this question is not different than asking the ethnicity question. We should never assume," Salyer says.

• Work with vendors to address gender billing issues.

If the billing process is manual, Salyer says to build electronic flags in the system to populate work queues, or build claim edits to catch these

accounts to reflect the proper gender for billing.

"Use regulatory language as a stepping-off point for your system vendors to change their systems to accept multiple gender codes, or to modify edits in the system for those traditional edits that may kick out due to gender-specific procedures," Salyer suggests. ■

REFERENCE

1. *Federal Register*. Nondiscrimination in Health Programs and Activities, a Rule by the Health and Human Services Department. Issued May 18, 2016. Available at: http://bit.ly/2qJzT30. Accessed May 5, 2017.

SOURCES

- **Melissa A. Salyer**, CRCR, Director, Patient Access, Chesapeake (VA) Regional Healthcare. Phone: (757) 312-6528. Email: Melissa.Salyer@chesapeakeregional.com.
- **Kathleen Shostek**, RN, ARM, CPHRM, Vice President, Healthcare Risk Management and Patient Safety, Sedgwick, Chicago. Phone: (312) 521-9252. Email: kathleen.shostek@sedgwick.com.

Registration Through the Eyes of a Transgender Patient

For a transgender person, navigating registration, scheduling, and billing aspects of healthcare is very complicated. **Ben Viohl** was born female but identifies as male, and has been on hormone replacement therapy for almost 10 years.

"Within that time frame, I have changed my gender marker and name legally, but I haven't had any surgery yet," Viohl says. Under state law, Viohl is unable to amend his birth certificate until that occurs.

"Because of that, my driver's license does not match my birth certificate. This would make me a male with a uterus," he explains.

This makes filling out registration forms difficult for a variety of reasons.

"The inconsistency leads to confusion. If filled out incorrectly, it tends to lead to insurance denial," Viohl says.

Some common examples: A transgender man may need screening for cervical cancer, needs a hysterectomy, or has uterine cancer.

"Is the hospital going to be able to register, code, and bill those procedures correctly? Will the hospital communicate correctly with insurance, or vice versa? These are concerns that the transgender community faces every day," Viohl says.

Additional Categories Needed

Miscommunication has led to delays in treatment, lab results, and insurance denying coverage for a service that is actually covered.

"It is vital that hospitals and doctor's offices educate themselves about transgender healthcare pitfalls," Viohl says.

Most registration systems allow only for "male" and "female" options when classifying the patient. Some transgender people identify as the gender opposite of their sex assigned at birth. Some do not identify as either, and some fall somewhere in the middle of the gender spectrum.

"I feel that categories in addition to male and female, such as 'transgender, transsexual, and/or other,' should be available choices," Viohl says. "This may allow for more flexibility when billing insurance."

Many states have laws restricting a transgender person's ability to change his or her gender documentation.

"Registration staff should be aware of this," Viohl says.

He would like to see registrars ask the transgender patient how they identify.

"I have found that if initial registration is performed in an open, informative, and respectful manner, there are fewer issues with insurance because the right questions are being asked," Viohl says. ■

Online Training Saves Money, Improves Productivity

About 90% of what occurs in her patient access department is automated, according to **Stefani Moore**. That includes training, much of which employees complete through online modules.

"This allows employees to self-access and take their assigned modules with 24/7 convenience. It accom-

modates all shifts and days of the week," says Moore, regional manager of patient access at St. Joseph Health in Irvine, CA.

With more than 300 team members across multiple campuses, **Tara Leigh Shorley**, MHA, SSGB, CHAM, relies heavily on online training.

"I find it very effective, mainly after we have had meetings to discuss changes," says Shorley, director of the Patient Access Services Contact Center at Baptist Health in Jacksonville.

Continual Updates

At St. Joseph Health, patient access leaders recently used online training modules for annual compliance training on patient privacy regulations and active shooter awareness.

"Every time we have changes and updates on policies, we send out a link, which allows the user access to the resource," Moore says. Online training is an easy way to update staff on ever-changing payer requirements, and inform them of any changes in departmental policies on self-pay patients and financial assistance. Despite the continual need for training, patient access staff still must maintain their productivity expectations.

"In addition to the flexibility of time, online modules allow employees to learn at their own pace for better understanding," Moore says.

The department also saves considerable costs by not spending funds on a trainer.

"Those resources can be directed in another manner," Moore notes. "It's also a greener way of communicating. We save money on paper for documents that would be disseminated."

However, the department's use of online training is limited in scope.

"We defer from online training when important new implementations come into place, which affects the entire staff," Moore says.

In-person training is a better approach for that type of comprehensive education.

"When management needs to ensure that there is overall understanding, we make ourselves available to answer questions and set expectations," Moore says. ■

SOURCES

- **Stefani Moore**, Regional Manager, Patient Access, St. Joseph Health, Irvine, CA. Phone: (949) 381-4685. Email: Stefani.Moore@stjoe.org.
- **Tara Leigh Shorley**, MHA, SSGB, CHAM, Director, Patient Access Services Contact Center, Baptist Health, Jacksonville, FL. Phone: (904) 202-1586. Fax: (904) 391-5746. Email: tara.shorley@bmcjax.com.

COMING IN FUTURE MONTHS

- Effective processes if ED patients lack identification
- React to social media complaints about patient access
- Prevent registration-related EMTALA violations
- Strategies for compliance training in patient access

HOSPITAL ACCESS MANAGEMENT™

HIPAA REGULATORY ALERT

CUTTING-EDGE INFORMATION ON PRIVACY REGULATIONS

What You Think You Know About HIPAA Might Be Wrong

Healthcare organizations take HIPAA seriously and typically devote substantial resources to education and monitoring, but misconceptions about the privacy law still can trip up the best efforts.

One of the most common misconceptions concerns when a healthcare provider needs a business associate agreement (BAA) with a vendor, says **Ira Parghi**, JD, an attorney with Ropes & Gray in San Francisco.

HIPAA requires covered entities, including hospitals, to put BAAs in place with their vendors in certain circumstances, but there is a fair amount of confusion as to what those circumstances are, Parghi says.

HIPAA requires a BAA if the vendor receives protected health information (PHI) from the covered entity to provide services to or on behalf of the covered entity, Parghi explains. The decision to frame a certain vendor relationship as a business associate relationship has important implications, she notes.

"The BAA, or other accompanying contract, must set forth a number of required elements, with the result that a BA relationship entails certain concrete contractual obligations. HIPAA also imposes certain duties, such as the requirement to have privacy and security policies, on BAs as well as covered entities," Parghi says. "And from an enforcement perspective, growing attention is being placed on BA relationships, with regulators often asking, for instance, how the covered entity has managed a particular BA relationship, or whether and how the BA has implemented its own training and policy requirements."

Both parties in a BA relationship must be prepared, organizationally and financially, to "manage to" the agreement, Parghi says, meaning they must organize their operations in such a way as to uphold their various contractual and HIPAA obligations, some of which can be quite resource-intensive.

> BOTH PARTIES MUST ORGANIZE THEIR OPERATIONS IN SUCH A WAY AS TO UPHOLD THEIR VARIOUS CONTRACTUAL AND HIPAA OBLIGATIONS, SOME OF WHICH CAN BE QUITE RESOURCE-INTENSIVE.

Some covered entities have erred on the side of requiring BAAs with all their vendors as a matter of course, without considering the specific nature of a particular vendor relationship. Consequently, such covered entities require BAAs from vendors that do not receive PHI from the covered entity (and are, therefore, not BAs), or who only come into occasional incidental contact with PHI while performing their work (and, therefore, fall under the HIPAA exception for incidental disclosures).

"We have seen healthcare institutions try to enter into BAAs with elevator servicing companies, cafeteria management companies, and the like, and in general, such relationships are not going to constitute BA relationships for HIPAA purposes," Parghi says. "On the other side of the spectrum, some covered entities do not require their vendors to sign BAAs when they should. For instance, vendors of electronic medical record platforms, and the companies that respond to patient requests for record copies on behalf of hospitals, are almost certainly going to be BAs."

Outside attorneys and other experts, collection

companies, photocopy companies, and practice support vendors may be BAs, depending on, for instance, the type of information disclosed to them, Parghi says. An attorney who assists on a corporate deal without ever seeing the names or any other information about patients likely is not a BA, but an attorney who provides advice on potential HIPAA breaches and reviews specific privacy incidents while conducting that work likely is.

A company that only photocopies financial records that have no patient information may not be a BA, but a company that photocopies clinical information likely is, she explains.

"Related to this, some covered entities have been known to sign BAAs provided to them by their vendors without carefully reviewing them, or to vary the terms of their own forms of a BAA too readily when asked to by a vendor, without weighing the request carefully. These approaches, too, can create risk," she says.

HIPAA also sets out certain exceptions to the BA requirement, Parghi notes. For example, exceptions may apply to vendors that are serving as "conduits" for PHI only, vendors who only come into incidental contact with PHI and take certain required precautions, and vendors who are healthcare providers to the patients in question. These also require fact-specific analyses, rather than assuming the answer.

"Whether a particular HIPAA exception to the BA requirement applies in a certain case, and what operational and other steps should be taken to ensure that that exception applies coherently, are questions that covered entities and vendors are urged to discuss with their legal advisors," Parghi says.

Legal advice also is a good idea when considering whether to carry out risk analyses under attorney privilege, Parghi says. There may be pros and cons to both approaches.

The popularity of concierge medicine, or the overall effort to make physicians more accessible to patients, increases the risk of HIPAA breaches via telephone, says **Andy Altorfer**, CEO of CirrusMD, a healthcare technology company in Denver. The physician may provide his or her cellphone number to the patient, giving little thought to the security of exchanging PHI in that way, he says.

"Sometimes, they have the patient sign a waiver, but that does not absolve your data security concerns," Altorfer says. "Texts are stored on non-secure telecom servers, with identifiable patient information and PHI. You don't have BAAs with those entities and they have no documented security or auditing, so typical phone texts will always be a fundamental HIPAA security breach."

HIPAA Security Rule compliance remains challenging for some healthcare providers, Parghi says. They often misunderstand the nature and scope of their obligations under the Security Rule, she says.

The Security Rule is organized into three sections that discuss the technical, administrative, and physical safeguards that a covered entity must carry out with respect to electronic PHI, Parghi explains. Each category of safeguards enumerates specific implementation standards, some of which are "required" and others of which are "addressable." All the implementation standards are "technology neutral," meaning that they do not mandate the use of specific technologies, she says.

"One common point of confusion for covered entities arises with the interpretation of 'addressable' implementation standards. Addressable standards, contrary to common perception, are not optional. They must be implemented if it is reasonable and appropriate to implement them," she explains. "And if the decision is made to not implement them, the decision should be appropriately documented. Unfortunately, some covered entities have misunderstood this requirement, and hence not approached these decisions and their documentation appropriately."

In addition, Parghi says healthcare providers sometimes fail to appreciate that many of the obligations arising under the Security Rule are ongoing obligations, not "one-time only" technological fixes. For instance, risk analyses under the Security Rule are supposed to be updated annually and also in the event of certain material changes, such as a change to a hospital's electronic medical record system.

"Regulators have sometimes asked for annual risk analyses from the years before, during, and after a breach, and providers who have not updated those risk analyses annually have found themselves penalized," she says. "Likewise, ePHI access and use is required to be monitored on an ongoing basis, and regulators may request evidence that, during a certain time frame, such access and use was properly monitored, and instances of potentially improper access or use appropriately investigated."

Misconceptions also can arise over the potential scope of Security Rule compliance investigations, which often are much more expansive in scope than one might expect, she says. Regulator inquiries may not just focus on the specific requirements in the Security Rule that are pertinent

to a particular privacy or security incident, more broadly assessing general compliance with Security Rule requirements. For instance, regulators may ask for copies of annually updated risk analyses, various policies and procedures, information about access controls, breach assessments, security logs, and the like, Parghi says.

"A healthcare provider undergoing a Security Rule investigation may find that, once the hood of the car is opened, much of it will be inspected," Parghi says.

Security Rule compliance is most effective when a range of stakeholders are included, Parghi says. Successfully implementing the various requirements under the Security Rule is an ongoing, and resource-intensive, process, she notes.

"In our experience, the healthcare providers who are most successful have generally been able to bring together important stakeholders from seemingly disparate functions in the organization, such as information security, compliance, information technology, and clinical risk management, and encouraged them to work cooperatively," Parghi says. "Too often, the only personnel who understand HIPAA are the ones who lack technological training, and the only personnel with technological expertise are not well-trained on HIPAA's Security Rule requirements."

Healthcare providers also can misunderstand what is allowed when providing patient information to clinicians, says **Heather Delgado**, JD, partner with the firm of Barnes & Thornburg in Chicago. Physicians sometimes request information on a patient and are told that it cannot be provided because of HIPAA restrictions, and Delgado says that almost always is not correct.

"There is a treatment exception in HIPAA that allows clinicians to share information about patients, but we still see clinicians refused and there is no reason for it," Delgado says. "When they block that access, that's actually when they're in violation of HIPAA because HIPAA fully states that you can share PHI for treatment purposes. This can come up often with specialty providers trying to get information on a patient, and it can be detrimental to the patient's care and safety."

Delgado notes that healthcare providers often assess the success of their HIPAA training by how well employees know when and how to protect PHI, without also assessing their understanding of when not to block access. This can lead to employees choosing to err on the side of caution and say no to data access when they are doubtful or just don't know if it is allowed, she says.

"A lot of the HIPAA mistakes you see could be prevented from the outset if there was proper training," Delgado says. ■

SOURCES

- Andy Altorfer, CEO, CirrusMD, Denver. Telephone: (720) 593-9549. Email: contact@cirrusmd.com.
- Heather Delgado, JD, Partner, Barnes & Thornburg, Chicago. Telephone: (312) 338-5905. Email: heather.delgado@btlaw.com.
- Ira Parghi, JD, Ropes & Gray, San Francisco. Telephone: (415) 315-1285. Email: ira.parghi@ropesgray.com.

HIPAA Not Just About High-tech Security

One of the most common mistakes is to perceive HIPAA compliance as solely or predominately a technology problem, says **Michael R. Overly**, JD, partner and privacy and data security lawyer at the law firm of Foley & Lardner in Los Angeles. He has heard administrators and other healthcare professionals say that their organization is HIPAA-compliant because the IT department has everything locked down with all the right software, encryption, and other technological solutions, as if that is enough.

"That is a problem, because if you look at the statistics in just the last year, two-thirds arose not from a technology failure, but rather human error," Overly says. "It is very hard to get people to start thinking about how HIPAA compliance is their responsibility and doesn't fall entirely on the technology side."

While some investment in technology is necessary, Overly cautions against the easy assumption that spending a lot on a software solution makes you compliant. That same $100,000 might have a bigger effect if it is spent on employee education, he says.

The goal should be to make information security a personal issue for individuals in healthcare, Overly says, but he admits that can be a hard sell. One way to get the message across is to show how understanding HIPAA security can help them in their personal lives, he suggests. He used this approach at a grand rounds presentation at a hospital, finding the audience much more receptive than they usually are to lectures on HIPAA compliance.

"You want to show them that if they grasp the key elements of HIPAA compliance, they can also benefit from that knowledge to protect their family photographs stored in the cloud, their tax records stored on their home computers, and their email accounts when they are under attack," Overly says. "When you explain to physicians that they might go home that night and find all their years of family photographs gone forever, you get them leaning forward. Then they will listen to how the same techniques that they can use to secure their data at home can also be effective in complying with HIPAA at work."

Another misconception is that HIPAA is all about confidentiality and security, Overly says. The component often overlooked is integrity — the validity and accuracy of the protected data, he says. This is where hackers are starting to focus more attention, potentially with ransomware attacks.

"We've seen ransomware attacks in which hackers take away our access to data and make you pay to get it back, but I worry that we're going to start seeing attacks on integrity of data, which could be devastating in healthcare," Overly says. "It's one thing if the hacker just has your data, and it's something else if that hacker says your data is going to be destroyed or hopelessly compromised. With people's healthcare information, that can have very serious consequences."

Overly also cautions that the backup tapes providers depend on to preserve PHI also could be exploited by hackers. People often assume that they have little to worry about if their data is backed up, but Overly says it is crucial to assure that those backups are not infected with malware or have security vulnerabilities.

"If you're subject to an attack, the first inclination is to just restore your data from a backup tape. What people don't realize is that hackers know that and sometimes will use malware that makes its way to your backups and then sits dormant for months until you try to use that tape," he says. "You would think that by now healthcare providers would be aware of that, but we're seeing that is not the case."

Few healthcare providers also have a plan for stopping a malware attack from multiplying, Overly says. If one clerk in accounting accidentally clicks an email link and infects that department's computer system, there should be an immediate response once that is detected, he says. An immediate and wide-reaching alert to every other department and all staff should notify them about that particular email or threat so they can avoid more infections, he says.

"An infection in the accounting department doesn't have to spread and affect every other part of the system. People assume that once it's in one time, that malware is spreading through the whole organization and that's not necessarily so," Overly says. "But if different departments are attacked, you can have multiple points of access for the malware and that makes the attack much more serious."

Another misconception is that HIPAA requires encryption of ePHI, says **Peter Tippett**, MD, PhD, chairman of DataMotion, a company in Florham Park, NJ, that provides security and compliance assistance to healthcare facilities. Although encryption is well-advised for any ePHI in transit or stored on mobile devices, it is not actually required by HIPAA, he says.

You could theoretically say you've performed a risk assessment and determined that the encryption is unnecessary, Tippett says.

"Encryption is all about making the data useless after a theft, so for your big mainframe computers, for instance, you might say that you have all kinds of extensive security with cameras, and cages, and locks, and so forth that makes the threat of theft very low with that hardware," Tippett says. "So, it would be reasonable in that instance to say you're not going to encrypt that stored data. I've seen that work a number of times, but it's not something most organizations would imagine doing."

Organizations also can emphasize technological security so much that the low-tech ways to violate HIPAA are overlooked, says **Dennis Deruelle**, MD, FHM, national medical director for acute services with IPC Healthcare/TeamHealth, a company providing healthcare professional staff and integrated care providers in Tampa, FL.

"We teach people about the risk from texting, hackers, and lost laptops, but you also have the low-tech breach where someone walks into a room and starts talking about something sensitive with the family or others present," he says. "That even happened to my wife. Her surgeon walked into the room and said, 'You have a little nodule on your lung,' in front of eight people." ■

SOURCES

- Dennis Deruelle, MD, FHM, National Medical Director, Acute Services, IPC Healthcare/TeamHealth, Tampa, FL.
- Michael R. Overly, JD, Partner, Foley & Lardner, Los Angeles. Telephone: (213) 972-4533. Email: moverly@foley.com.
- Peter Tippett, MD, PhD, Chairman, DataMotion, Florham Park, NJ. Telephone: (800) 672-7233. Email: info@datamotion.com.