FOR MORE THAN 30 YEARS

HOSPITAL ACCESS MANAGEMENT™

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

SEPTEMBER 2017 Vol. 36, No. 9; p. 97-108

INSIDE

AHC Media
A RELIAS LEARNING COMPANY

Are Payers Meeting Their Own Requirements for Auths? Find Out What Contractual Language Says

Exact wording gives more "ammo" for appeals

A claim is denied because the payer was not notified of the patient's admission within 24 hours. At first, it seems pretty clear that the claim won't be paid, since the required timeframe was not met.

"However, there have been times when we look at our contracts, and we find out that we actually have a 48-hour window to notify the payer of the admission," says **Suzanne Droste**, MBA, director of access services at UW Health in Madison, WI.

"SERVICES ARE MEDICALLY NECESSARY, BUT ARE DENIED BECAUSE OF NO AUTHORIZATION."
— JENNIFER LANTER, THE OHIO STATE UNIVERSITY WEXNER MEDICAL CENTER

Armed with this knowledge, patient access has appealed many denied claims successfully. "Before, we may have written off these charges, assuming we missed the notification deadline," says Droste. "We have realized that insurance company customer service reps generally quote their *standard* contract language."

The hospital's specific contract with the payer is sometimes different. "Knowing the requirements specific to our contracts has been key," says Droste. "This has given us more knowledge and 'ammo' when appealing denied claims."

Recently, patient access leaders met with the contracting department to get this information. "The first takeaway from this collaboration has been a handful of plain language contract summaries from our top payers," says Droste. Specific wording from contracts about notification requirements has proven to be very valuable for patient access.

"We can tell them what our contract says, and feel confident in our appeals," says Droste. "We are much more

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
EXECUTIVE EDITOR: Leslie Coplin
EDITOR: Journey Roberts
AHC MEDIA EDITORIAL GROUP MANAGER: Terrey L. Hatcher

AHC Media
A RELIAS LEARNING COMPANY

successful." (*See related story on the patient access department's denials management team.*)

Time Spent Is 'Enormous'

"No authorization" is a top reason for denied claims at The Ohio State University Wexner Medical Center. "It currently represents about 22% of our denial challenges that result in lost net revenue," reports **Jennifer Lanter**, MSPH, BSN, RN, CCRC, director of revenue cycle clinical support.

Payers currently set their own response timelines. Some take up to 30 days to respond to an authorization request.

"We spend an *enormous* amount of time following up on requests to determine the status," says Lanter.

Typically, payers don't respond until the end of their timeframe. Sometimes, patients must be rescheduled only because a payer has not responded to the requests for authorization in time.

"We push back all of the time by frequently calling to indicate when we need a response," says Lanter.

Payers don't always meet their timeframes. In these cases, says Lanter, "we escalate through our managed care department, if we are contracted with the payer."

Retro Auths Disallowed

Getting authorizations for "stat" or same-day requests is particularly challenging for patient access. "We spend time trying to secure the authorization before the services are rendered. But taking care of our patients is our highest priority," says Lanter.

The hospital provides urgent services regardless of the authorization status.

"We attempt to capture these through a work queue in order to obtain retro authorization," says Lanter.

To successfully appeal denied claims, good documentation of medical necessity is needed. Often, however, the payer is not disputing that the patient needed the service — only the fact that the authorization was not in place before the service was provided.

"We are frequently frustrated," says Lanter. "The services are medically necessary, but are denied because of no authorization."

Requirements Unmet

Payers continuously change their authorization requirements throughout the year. The verification process varies, too.

"Payers have a multitude of ways to verify authorization requirements,"

EXECUTIVE SUMMARY

Patient access departments are using contractual language to overturn unfairly denied claims. Take the following steps to challenge payer requirements:

- Ask the hospital's contracting department for education on payer contracts.
- Find out if requirements conflict with what is stated in the contract.
- Include contractual language in appeal letters.

Nurses Stay on Top of Auth-related Denials

Constantly changing payer requirements are a top pain point for patient access departments.

"It is difficult to stay on top of all the notification deadlines, prior auth requirements, and timeframes to appeal denials," says **Suzanne Droste**, MBA, director of access services at UW Health in Madison, WI.

UW Health recently created a small denial management team within the prior authorization department. "We are in the early stages of building this team," says Droste. "We are continually finding ways to improve and expand."

This team currently consists of two nurses who handle prior authorization-related denials. "These are not new FTEs. We have slowly built this team from existing resources," Droste explains. Previously, both of the nurses worked as pre-certification nurses.

The group also handles denials related to patient classification. For instance, the hospital may bill as inpatient status, but the payer says only observation status is appropriate. "The nurses research the case, appeal the denial if appropriate, and keep tabs on the final outcome," says Droste.

Most of these cases take a long time to review. "It requires digging into the chart for clinical information to support inpatient classification that we have not yet provided to the payer," Droste explains.

The denial management nurses spend a lot of time gathering information to include in detailed appeal letters.

"We are most successful when we can tell the entire story, using clinical information to back it up," says Droste. ■

explains Lanter. For some, entering a CPT code on the payer website is sufficient. Other payers require a time-consuming phone call.

Requirements differ based on the level of service — inpatient, outpatient, or observation. "Or they may have medical policies that state a service is only covered when certain conditions are met," says Lanter. Payer representatives do not always include this information during calls.

To stay on top of things, patient access must review each payer's website continuously for new authorization requirements. Anytime there is a new requirement, process changes are necessary.

"As you can imagine, requirements may slip through the cracks," says Lanter. Recently, "no auth" denials have been occurring for devices. "Historically, an authorization for a procedure covered the device used in the procedure," says Lanter.

For instance, authorizations for a cochlear implant covered both the procedure and the device. Payers now require separate authorizations for both the procedure *and* the device.

"This has required us to develop a completely new workflow to include the device codes in the authorization process," says Lanter.

Issues like this are identified when patient access reviews monthly data to identify the root causes of denied claims. "We reach out to the departments performing the services to fix operational processes," says Lanter. "We make changes to our system workflows when new services require authorization."

Patient access updates tip sheets and educates ordering physicians on additional documentation that is needed. "We are also looking at additional tools to assist with managing the continually changing payer authorization requirements," says Lanter. ■

SOURCES

- **Suzanne Droste**, MBA, Director, Access Services, UW Health, Madison, WI. Phone: (608) 263-6915. Email: sdroste@uwhealth.org.
- **Jennifer Lanter**, MSPH, BSN, RN, CCRC, Director, Revenue Cycle Clinical Support, The Ohio State University Wexner Medical Center, Columbus. Phone: (614) 293-2115. Email: jennifer.lanter@osumc.edu.

Auth Doesn't Match Service? Expect Claim Denial

Lost revenue, surprise medical bills

Once a physician puts in orders for a patient, patient access jumps into action. Registrars do everything possible to secure authorizations and ensure payment for the provider and the hospital.

But what if the Healthcare Common Procedure Coding System (HCPCS) or CPT (Current Procedural Terminology) codes are incorrect?

"I don't think physicians fully

EXECUTIVE SUMMARY

Claims denials often occur as a result of "mismatches" between what was ordered or scheduled, and what actually was done. The following steps will help ensure payment:

- Schedule tests only if the authorization is in place.
- Confirm that correct codes are in place before authorization is requested.
- Include multiple codes in orders if possible.

understand when they order these tests how manual hospitals are in making sure that the test done matches the authorization," says **Suzanne Lestina**, CPC, FHFMA, vice president of revenue cycle innovation in the San Diego office of Avadyne Health, a provider of revenue cycle management services.

For example, the physician schedules a CT of the brain with contrast, and registration gets the authorization. The order goes through to radiology, but no one notices that the physician added an MRI or other test.

"Nobody says, 'The authorization doesn't match,' until the pieces are put together on the billing side," says Lestina.

A surprising number of claims denials happen because of this very common scenario. "It's a whole process breakdown," says Lestina. "Hospitals really need to engage key stakeholders in understanding this."

The resulting lost revenue can be devastating to the many hospitals that are struggling financially. "Many of the clients I deal with are on hiring freezes," notes Lestina. "Why do we have a process that results in lost revenue?"

Different Test Done

A patient needs a CT of the brain without contrast, and the test is scheduled. Patient access obtains an authorization for that test. However, when the physician writes up the actual order, he orders a CT of the brain *with* contrast. "So the test that's ordered differs from the CPT code of the test that's called in. And nobody sees that it's incorrect," says Lestina.

Registration typically doesn't have access to the patient's medical records to view the actual order. Radiology has no way to see that the order they receive is different from what was authorized.

"The doctor is treating patients, and is not thinking along those lines," says Lestina. "Nobody stops to think, 'This is different.' There are lots of opportunities for this to fall through the cracks, and it happens all the time."

Requests for tests can come from both the physician's office and the patient. "In both cases, the test is scheduled even if an actual order wasn't received yet," says Lestina. Patients are asked to bring the order with them, but registrars rely on the patient's interpretation of what test is needed. In other cases, registrars take verbal orders from the office staff, and ask to have the order sent over.

"If it's not matched with the test that was just scheduled, and it's not compared, then registration staff are following up on an authorization that is potentially for the wrong service," says Lestina.

THE OBVIOUS PROBLEM IS THAT PAYERS CAN AND DO REFUSE TO PAY IF THE AUTHORIZATION WAS NOT OBTAINED PRIOR TO SERVICE.

A 'Huge Dissatisfier'

If patients show up for a test without an authorization in place, hospitals generally allow them to have the test done anyway.

"Hospitals balk at turning the patient away. They want to get the patient through, and then get the authorization," says Lestina. "People have to understand the ramifications of this."

The obvious problem is that payers can and do refuse to pay if the authorization wasn't obtained prior to service.

"It doesn't do anybody any good if the patient has the test, but the hospital has to write it off or the patient has to pay for it," says Lestina. "That's a huge dissatisfier."

To ensure payment, tests would be scheduled only if the authorization is in place *and* the CPT or HCPCS code matches. When the physician's office calls to schedule a patient for an MRI, registration should ask for the authorization number. "If there is none, the response should be, 'Call me back, and we'll schedule it the minute you do,'" says Lestina.

If a test is done with contrast, but

the authorization is for a test without contrast, "the patient is caught in the middle of the broken process," says Lestina.

Ideally, radiology would immediately notify patient access if a different test is done. "But I don't know anybody who's actually doing that," says Lestina. "It's a huge cultural thing. It's bringing the clinical and financial sides together."

Catch 'Mismatches' Before Denial Is Triggered

Patient access leaders at Moffitt Cancer Center in Tampa, FL, created a worklist to capture "mismatches" in authorizations that were causing claims denials.

"Our system identifies all the high-tech radiology tests that have already been financially cleared, but the order has changed. These encounters are routed to a unique list," says **Viviana Mahon**, manager of the financial clearance unit.

A team member from the financial clearance unit identifies if the new test is covered under the current authorization number. If it's not, the insurance company is contacted for an updated authorization.

"This worklist is worked in full no later than the date of service," says Mahon.

As a result of this new process, the hospital no longer sees denials on surgical cases due to discrepancies between the authorized procedure and the performed procedure. Mahon estimates that denials have decreased by 24% overall, in part because of the new protocol.

Once the physicians order a surgical case, the coder in the financial clearance unit reviews the order and assigns the proper codes *before* authorization is requested. "This avoids denials in the back end," says Mahon.

At Salt Lake City, UT-based Huntsman Cancer Institute, the patient access department set up a workflow just for stat or same-day add-on orders. "The preauthorization team can initiate the auth process right away — although some plans won't grant approval timely," says **Junko I. Fowles**, CHAM, supervisor of patient access and financial counseling.

When that happens, financial counselors and ordering providers get involved for urgent peer-to-peer reviews. If necessary, they give patients the option of paying out of pocket for the test. "The appropriate procedure may not be determined until the patient actually goes into the OR, or until same-day lab tests are run, in the case of chemotherapy," says Fowles. Sometimes surgeons put in the order in the form of "CPT XXXXX vs. XXXXX"

Fowles explains, "The pre-auth team is able to submit both codes to the insurance medical review team, when the actual procedure being performed could be 'either/or.'" ■

SOURCES

- **Junko I. Fowles**, CHAM, Division of Revenue Cycle Support Services, Huntsman Cancer Hospital, Salt Lake City, UT. Phone: (801) 587-4036. Fax: (801) 587-8269. Email: Junko.fowles@hsc.utah.edu.
- **Viviana Mahon**, Manager, Financial Clearance Unit, Moffitt Cancer Center, Tampa, FL. Phone: (813) 745-1937. Fax: (813) 449-8869. Email: viviana.mahon@moffitt.org.

$6 Million in Write-offs

Lestina often discusses the issue of mismatched authorizations with her hospital clients, but it is hard to overcome. "Often, hospital administrators or clinical areas don't see the process as part of the patient's experience," she explains.

Even at hospitals with entire departments dedicated to obtaining authorizations, mismatches between what was ordered and what was authorized are not caught. At one hospital, authorization write-offs totaled $6 million in one year. Lestina identified these two problems that were contributing to the write-offs:

- Frequently, patients were not rescheduled, even if the authorization was not in place.
- Patient access relied on the physician to conduct the peer-to-peer review if required by the payer. There was no follow-up to ensure the authorization actually was secured.

"Employee physicians are easier to get on board," says Lestina. "Physicians in the community are harder to engage."

By collaborating with radiology, patient access can close "information gaps," says Lestina. "Walk through what currently happens — a day in the life of an authorization — and identify where all the gaps could appear." (*See related story on how patient access can fix "mismatches."*) ■

SOURCE

- **Suzanne Lestina**, CPC, FHFMA, Vice President, Revenue Cycle Innovation, Avadyne Health, San Diego. Phone: (619) 819-8844 ext. 1053. Email: slestina@avadynehealth.com.

Educate Registrars and Patients on New Medicare ID Cards

Concern over identity theft has made patients understandably reluctant to give their Social Security number to registrars, especially over the phone.

"This greatly impacts the ability to correctly identify patients during scheduling and pre-registration processing," says **Sandra J. Wolfskill**, FHFMA, director of healthcare finance policy at the Healthcare Finance Management Association.

As of April 2018, the Centers for Medicare & Medicaid Services will start mailing new cards to people with Medicare benefits. The cards will have a new unique, randomly assigned number called a Medicare Beneficiary Identifier (MBI), to replace the existing Social Security-based Health Insurance Claim Number (HICN). All Medicare cards will be replaced by April 2019.

"It is going to be mission critical that *all* provider systems that currently use or record the Social Security number have the ability to capture and store the new number," says Wolfskill.

It's not enough to simply replace the Social Security number with the MBI. "Both the social security number currently in the patient's record, as well as the new MBI, should be captured and stored," Wolfskill explains.

Training Will Be Essential

Patient access staff need to understand the new MBI system, as well as where to place the number in the various records. "Staff also need to be prepared to explain this identifier change to patients," says Wolfskill. Patient access staff will need to do these three things:

1. Ask the beneficiary if he or she has received a new identification card from Medicare recently.

2. Describe the card. "Beneficiaries will not recognize the new card as an 'MBI.' So eliminate initials and acronyms from the conversation," says Wolfskill.

3. Explain that the new card is designed to protect their privacy.

"It is important to remember that this is a phased-in change. Some beneficiaries will not have a new card for a number of months," says Wolfskill.

Revenue cycle leadership will need to plan how the use of the Medicare number on claims will migrate to using the new MBI number system.

"Make sure staff understand why the identification numbers are being changed," emphasizes Wolfskill. "Caution against the use of initials or acronyms!"

An equally important step: Identify *all* systems that need modification. "If you are using a bolt-on tool for insurance verification, for example, is your vendor making the appropriate changes to that system?" asks Wolfskill.

The best approach is to get staff involved in creating scripting for this change. "The final script needs to sound natural and be easily understood by the beneficiaries," says Wolfskill. Giving staff an opportunity to practice the new scripting in a classroom or meeting well before the initial implementation begins is ideal.

Patient access departments will need to make these other changes, says Wolfskill:

1. Quality data edits will need to be modified.

"At the end of the 21-month implementation schedule, every account needs to be validated for the new MBI," says Wolfskill.

2. Patient access leadership will need to review all systems, written and electronic forms, and correspondence to ensure that the new MBI number replaces the patient's current Medicare number.

"Obviously, the EHR will require modification to retain the old HICN, but also capture the new MBI as that information is collected," says Wolfskill.

3. Any subsystem, such as Advance Beneficiary Notice production, also will need to be modified to capture and print the new number.

Likewise, supplemental payers currently using the HICN as a patient

EXECUTIVE SUMMARY

Patient access departments need revamped processes to prepare for new Medicare ID cards without Social Security numbers. It is important to train staff on the following items:

- Where to place the number in records;
- How to explain the change to patients;
- How to use scripting well in advance of the change.

identifier will need to change their systems to accept the new MBI.

"Identifying those payers and testing claims with them is also important," adds Wolfskill. ■

SOURCES

- **Sandra J. Wolfskill**, FHFMA, Director, Healthcare Finance Policy/ Revenue Cycle MAP, Healthcare Finance Management Association, Westchester, IL. Phone: (708) 531-9600. Fax: (708) 531-0032. Email: swolfskill@hfma.org.

Are Registrars Going 'Rogue'? Effective Ways to Prevent Collection Complaints

Give excellent service while collecting

"They want us to collect, but when a complaint goes to the CFO or CEO they don't have our backs."

Registrars might not admit they feel this way, but many have expressed this sentiment to **Brandi Nash**, a revenue cycle consultant at Warbird Consulting Partners in Atlanta, GA.

"We are holding them accountable, but then we, as leaders, are not standing up for them," says Nash.

Upfront collections do not need to conflict with customer service, however. "The expectation needs to be across the board at all levels in your facility," says Nash. "If you receive a service, the expectation will be that payment will be discussed at the time of service."

Problems come if registrars are expected to collect, but aren't supported if patients complain about it. "This is a huge deal breaker for your front-end associates," says Nash.

An uptick of complaints about collections could signal a bigger problem than just one interaction that went wrong.

"Some clients are overly aggressive in the patient access area, due to the demands coming from the C-Suite," says Nash. "Finding the right balance is difficult."

Patient access leaders should hold registrars accountable for collecting. "But we don't want to create associates who are only focused on the money and lose sight of patient care," says Nash.

Having solid scripting for the collections conversation is helpful. "It decreases the chances of the associate going 'rogue,'" Nash explains. "The associate has less opportunity to be overly aggressive in demanding payment."

Even if a registrar is following guidelines and scripting to the letter, there are still times when he or she will be unable to collect. Nash goes by the "80-20" rule for collections: "As leaders, we have to accept the 20% of not collecting, but do a robust job on collecting the 80%."

Start Conversation Early

Joyelle T. Chrysostom, manager of financial clearance operations at Albany Medical Center, says registrars hear complaints about collections on a daily basis. Common comments are "I've never been asked to pay before," and "It's poor customer service to collect when someone is sick."

"The key is to communicate any financial responsibility to patients early in the revenue cycle," says Chrysostom. For instance, financial conversations begin while the patient is still in the ED for patients being admitted.

"We advise the patient that he or she may have a copay or deductible," says Chrysostom. If the patient is informed of this before going to the floor, he or she is less likely to send the credit card home with a family member. Sometimes, the mere mention of a copay spurs the patient or family to call the insurance company to confirm their financial responsibility.

"It is critical to let patients know that we are here to service them, and that options are available," says Chrysostom.

These include payment plans, Medicaid screening, or financial

EXECUTIVE SUMMARY

A growing emphasis on upfront collections occasionally results in dissatisfied patients. Patient access leaders can take the following steps to mitigate collection-related complaints.

- Support registrars if patients do complain.
- Start financial discussions as early as possible in the process.
- Give registrars scripting so they can be confident in asking for money.

aid. "We also offer to collect over the phone from a family member on behalf of the patient," says Chrysostom.

Projecting Confidence

Despite the growing practice of point-of-service collection, many patients still say, "I never had to pay upfront before." Registrars at Shasta Regional Medical Center in Redding, CA give this response: "We realize you may have not been asked in the past. But based on your benefits, our department is now required to collect upfront."

"If patients express they can't make a payment, we ask if they can pay anything toward the deductible. If not, we move on and still provide exceptional customer service," says **Kim Rice**, director of patient access. Rice says patient access staff need to understand these two things:

- The overall revenue cycle process;
- The advantages of collecting upfront — both for the patient and the organization.

Patient access staff need to understand what they are asking for and why. "When clerks can answer questions, it provides that extra confidence the patient needs to see," says Rice.

The opposite is true if the registrar doesn't know why he or she is asking for money or seems inexperienced.

"The patient can usually get out of paying easily — and it doesn't confirm their sense of confidence in the facility as a whole," says Rice.

Patients Want to Know

A little bit of education during registration or preregistration helps patients understand why upfront collections happen more today than in the past.

"In my experience, when you explain to patients what you are doing, they are open to your explanation," says Rice.

When patients do not understand why staff are collecting or their questions are not answered, they are more inclined to complain.

"It is important that the staff know to ask for assistance if they sense a problem with the patient," says Rice. This prevents things from escalating to the point where the patient feels the need to complain to someone.

"People, in general, want to know what they are paying for," says Rice. Scripting and thorough explanations are needed.

"We let the patient know there is an amount due based on their insurance benefit, and what the payment is for," says Rice.

Many patients ask what their out-of-pocket costs will be. This is not always an easy question to answer. "We are limited to the tools we have to give a specific amount," says Rice. "Sometimes, management must step in and provide extra guidance."

One patient wanted to know a definite amount. He didn't believe the registrar, who told him only an estimate was possible. "I met with the patient and explained that we really don't know how the insurance would process the claim," says Rice.

Rice then told the patient what was known for certain about his out-of-pocket costs. To give a good estimate, it was necessary to know the type of service, the benefits for that service, if the deductible had been met, and whether the patient had any other health visits in the calendar year that would have gone toward the maximum benefits of his coverage.

"Once I explained the details, the patient was satisfied and continued with the service," says Rice. ■

SOURCES

- **Joyelle T. Chrysostom**, Manager, Financial Clearance Operations. Albany (NY) Medical Center. Email: chrysoj@mail.amc.edu.
- **Brandi Nash**, Warbird Consulting Partners, Atlanta, GA. Email: bnash@warbirdcp.com.
- **Kim Rice**, MHA, Director of Patient Access and Communications, Shasta Regional Medical Center, Redding, CA. Phone: (530) 229-2944. Fax: (530) 244-5185. Email: krice@primehealthcare.com.

Training and Tools Can Stop Duplicate Medical Records

Accurate patient identification *always* has been critical to providing the best patient care. "But in today's digital medical record world, how do you properly identify patients who have common names or are unable to identify themselves?" asks **Kelly Clasen**, senior director of business operations at Middle Park Medical Center in Granby, CO.

Despite growing focus on the problem of duplicate medical records, the problem continues. "Hospitals all over the country are struggling with this daunting task — not to mention

EXECUTIVE SUMMARY

Patient access departments are using education and technology to prevent the creation of costly and dangerous duplicate medical records. Consider these strategies to help prevent duplication:

- Avoid rushing during the registration process, even during volume surges.
- Ask patients to spell their names instead of making assumptions.
- Meet with health information management to discuss ways to avoid duplicates.
- Implement consistent policies organization wide.

the safety and financial ramifications that can occur if a patient is actually misidentified," says Clasen.

According to the ECRI Institute, 7-10% of patients are misidentified when their Enterprise Master Patient Index (EMPI) and electronic health records (EHR) are searched. Of this group, 9% experience an adverse event. According to a report conducted by the American Health Information Management Association (AHIMA), between 8% and 12% of EHR records are duplicates.[1]

"Still more patients may suffer medical errors due to missing health information in their records, or overlays that mingle multiple patients' records together," says Clasen. Below are some common factors causing duplicate medical records.

- Traditional patient identifiers, such as oral demographic data, Social Security numbers, and patients' addresses, can be mistyped easily.
- Patients do not always give correct demographic information, and registrars sometimes fail to verify what they're given.
- Duplicates often are caused by patient access employees rushing during the registration process, in order to meet productivity goals or because patient volume is high.

Lesley Kadlec, MA, RHIA, CHDA, director of HIM (health information management) practice excellence at AHIMA, acknowledges, "There may be pressure to get the patient registered quickly in the hospital setting."

Family members or caregivers sometimes provide information to registrars on behalf of the patient, but don't know exact birthdates, middle initials, or insurance information. These identifiers may be important to match patients with their health information.

"Hospital registrars may also face language or communication barriers with patients or their family members," says Kadlec. Patients who are extremely ill, upset, or confused may be unable to provide accurate information.

"In emergent situations, where the need for timely treatment of the patient is most critical, hospital registrars may have no other option but to rely on incomplete information," says Kadlec. Registrars create a new patient record to allow the patient to get needed care as quickly as possible, and sort it out later.

Some patients use multiple names, shortened versions of their full name, or an initial for the first name with a full middle name. Others go by a nickname that is not similar to their legal name.

"These aliases have the potential to lead to creation of an EMPI duplicate," says Kadlec. This is particularly common in the hospital setting, because the patient usually is not known by registrars.

Common surnames and variations in spellings also occur. "It is not unusual to have multiple patients with the same or similar first, middle, and last names, who are near the same age, often related, and sharing other identifiers," says Kadlec.

Consider 'Downstream' Departments

Cleansing inaccurate patient records can be costly for hospitals. Clasen notes, "The average cost to resolve a single duplicate medical record is $100. If 8% of a hospital's records are duplicates, the costs to clean their EMPI database and EHR records increase exponentially."

At Longmont United Hospital, where Clasen was director of business services, the duplicate medical record rate decreased from 7% to 2% after palm vein recognition was implemented.

"This can not only improve overall patient safety and experience, but also improve financial outcomes," says Clasen. Costly cleansing of duplicates and overlays were reduced, as were denied claims resulting from misidentification.

However, patient access should not rely solely on biometric technology. **Adria Jones**, special projects coordinator at Harris Health System in Houston cautions: "Employees still need to interview the patient."

Registrars often assume they know how to spell the patient's name just based on how the name sounds. Instead, says Jones, "Ask patients to spell or write out their name."

Patient access employees need to be reminded continually of the

importance of doing a thorough search of the patient's medical record number.

"Emphasize the impact it has on patient safety, revenue delays, and time spent by all 'downstream' departments, such as HIM, to correct duplicate medical records," says Jones.

The following steps are taken at Harris Health:

• HIM reviews the duplicate medical record report and analyzes the potential reason for it.

• HIM sends a weekly report to the management team of each department on all duplicates that occurred in that area.

• Management educates the involved employees.

HIM created a patient search tip sheet specifically for patient access. "This explains the different way to search a patient in our system," says **Latrescia Brodie**, RHIT, CHIT-PW, EMPI/HIM manager at Harris Health System. (*See the steps taken by the patient access department.*)

HIM meets with patient access regularly to discuss duplicates and how to avoid them. "In a nutshell, communication, education, and good policies are the key tools to avoid creating duplicate records," says Brodie.

Kadlec would like to see the creation of a national patient identifier that could be used by multiple providers and healthcare organizations: "This would enable accurate patient matching whenever information is exchanged."

At the organization level, Kadlec says consistent policies and procedures "lay the critical groundwork for correct patient matching."

A data integrity team can review and remedy duplicates and overlays in patient health records. "Timeliness is important in this work," says Kadlec. "The data integrity team should quickly identify, review, and correct patient identification problems." ■

Use These Steps to Search for Patients

Creating new medical record number is last resort

Patient access employees at Harris Health System in Houston, TX, follow these steps to search a patient in the system:

STEP 1: Is the patient new or returning? Ask the patient if he/she has been seen at any of the hospital facilities.

• If Yes, go to Step 2.

• If the patient says No, still conduct a search for the patient before creating a new record. This is because the patient could have called the appointment center in the past but was never seen at any facilities. Use Step 2.

STEP 2: Proper patient name searches. Access the patient by using the following methods. Don't assume you know how to spell the patient's name. Ask the patient the spelling of their name.

• *Use the "3, 3" Process:* Enter the first three letters of the last name, a comma (,), and the first three letters of the first name. Also enter the sex and date of birth. This will bring up a list of patients. Review this list to identify cases with other matching data elements, as the patient may have multiple medical record numbers.

• Add additional letters to the first and last name and other known data elements, such as the patient's Social Security number, to narrow the search.

• Make sure all patients are loaded by using the scroll bar located on the right side. Before selecting the patient, make sure the demographic elements match the patient in front of you. If not, verify the demographic elements with the patient.

• If unable to locate the patient, ask the patient if he or she goes by another last or first name.

• If the patient isn't present and you're unsure how to spell the patient's name correctly, enter the full patient name (click the "Sounds Like" box).

• If the patient says he or she has been seen at your facilities and you are unable to locate the medical record number, proceed to Step 3.

STEP 3: Contact HIM. *(Enter HIM contact number and hours of operation)*

• If HIM is unable to locate the patient or you're unable to contact someone in HIM, go to Step 4.

STEP 4: After you have exhausted all search options, create a new medical record number.

REFERENCE

1. http://perspectives.ahima.org/wp-content/uploads/2016/03/WhyPatient.pdf.

SOURCES

- **Latrescia Brodie**, RHIT, CHIT-PW, EMPI/HIM Manager, Harris Health System, Houston. Phone: (713) 873-0759. Email: Latrescia_brodie@harrishealth.org
- **Kelly Clasen**, Senior Director, Business Operations, Middle Park Medical Center, Granby, CO. Phone: (307) 699-2413. Email: KClasen@mpmc.org.
- **Adria Jones**, Special Projects Coordinator, Harris Health System, Houston, TX. Phone: (713) 566-6712. Fax: (713) 440-1258. Email: Adria.Jones@harrishealth.org.

Quickly Update Patient Access About Changes

Convey important information to multiple registration locations

Simply reaching everyone in the department is the biggest training challenge for **Orlando Melendez**, system manager of patient access at Edward-Elmhurst Health in Naperville, IL.

Today's patient access departments face constant changes that need to be conveyed quickly across the entire organization. "The healthcare industry is highly regulated, rapidly changing, and complex," says Melendez.

Patient access staff are located at 25 different points of registration in 15 locations. "This makes it difficult to reach each staff member in person. We rely on email communication for delivery of training material," he says.

Melendez has found these approaches effective:

- Require staff to complete an attestation to confirm that they have reviewed the material.
- Include a short test to ensure staff comprehend the information.
- Relate the training topic to the staff member's role in the department.
- Explain the downstream effect of the process.
- Use lead and supervisor-level staff to deliver training material one-on-one or in small groups.

"Typically, this delivery method is reserved for new processes or for time-sensitive topics," says Melendez.

Insurance eligibility was a recent topic. The revenue cycle educator explained how doing this correctly connects with the patient's experience.

"If staff correct any discrepancies at the time of service, the patient won't end up getting a surprise bill," says Melendez.

Give Info Repeatedly

"Repeat, repeat, repeat" is the mantra of **Aimee Newson**, senior director of patient eligibility for Atlanta-based nThrive. She offers four steps to convey a process change to the entire patient access team:

1. Notify everyone by email, asking them to electronically sign to confirm receipt.

2. Follow up with an online update, allowing for interactive discussion if needed.

3. Test employees to determine their level of understanding.

4. Conduct internal quality auditing, to be sure the process change is actually being implemented.

"Everyone interprets what they are hearing a different way and change can be difficult for some," notes Newson. "It is important to validate changes are occurring."

Newson has assisted many patient access departments in compliance with 501(r) requirements. These require hospitals to make reasonable efforts to determine if an individual is eligible for assistance under the hospital's financial assistance policy.

"The training challenge is getting the patient access team to understand what 501(r) means to them, and incorporating it in their day-to-day work," says Newson.

Patient access must do two things.

- Ensure patients are offered financial assistance when they have limited ability to pay.
- Consistently follow the hospital's financial assistance policy.

Periodic auditing ensures this is done consistently, says Newson: "Identify trends in those patients tagged with financial assistance and auditing self-pay accounts notes."

EXECUTIVE SUMMARY

Patient access frequently needs to update all employees across the entire department quickly. Below are some strategies for time-sensitive training.

- Use leads and supervisors to deliver material one-on-one or in small groups.
- Have registrars confirm they've reviewed the material.
- Give information repeatedly.

Reach All Registrars

Kaniesha Mason, CHAM, associate director of patient access services at Syracuse, NY-based Upstate University Hospital, struggles to keep the entire department updated on payer requirements.

"It is always challenging to stay ahead of these changes in time to get proper notification out to the end users," she says. It's also difficult to pull all employees from their registration locations for classroom setting training. The department also has to train both centralized and decentralized registration staff.

"Since not all registrars work for patient access services, it can be challenging to hold all staff equally accountable for thorough registrations," says Mason. The department uses these strategies:

• "Lunch and learn" sessions cover new processes or clarify existing processes.

"For employees who are unable to attend in person because of coverage, these sessions are also posted as mandatory training, with a short proficiency exam to test their knowledge," says Mason.

• A registration-related article is included in the monthly departmental newsletter, which is reviewed at staff meetings.

• Employees regularly meet for 15 minutes with a supervisor.

"This provides an opportunity for staff to ask questions or demonstrate proficiency on any topic," says Mason.

• Cross-trained staff cover both emergency departments and central registration sites.

"We are able to share staff during peak times, and schedule more end users for face-to-face training," says Mason. ■

> IT IS DIFFICULT TO PULL ALL EMPLOYEES FROM THEIR REGISTRATION LOCATIONS FOR CLASSROOM TRAINING.

SOURCES

- **Orlando Melendez**, Director, Central Scheduling and Patient Access, Edward Hospital and Health Services, Naperville, IL. Phone: (630) 527-7472. Fax: (630) 548-7712. Email: omelendez@edward.org.
- **Kaniesha Mason**, CHAM, Associate Director, Patient Access Services, Upstate University Hospital, Syracuse, NY. Phone: (315) 464-9367. Fax: (315) 464-4005. Email: BarnettK@upstate.edu.

COMING IN FUTURE MONTHS

- Update on legislation on payer requirements for authorizations
- Start financial discussions much earlier in the process
- Effective responses if someone complains about registrar
- Avoid lost revenue due to mistakes with insurance eligibility

HOSPITAL ACCESS MANAGEMENT™

HIPAA REGULATORY ALERT

CUTTING-EDGE INFORMATION ON PRIVACY REGULATIONS

Myriad State Requirements Complicate Breach Response

When you realize there has been a breach of protected health information (PHI), your first thought is of HIPAA and how to satisfy federal requirements for responding. But that is far from the end of your obligation, as state requirements can be just as onerous.

And if you do business in more than one state, the response can be especially burdensome because state laws requiring data breaches can be radically distinct — each requiring something different and, in many cases, specifically tailored to that state's government, notes **Nathan A. Kottkamp**, JD, a partner with the law firm of McGuireWoods in Richmond, VA.

Alabama and South Dakota are the only states that don't have data breach notification laws.

"There is a crazy quilt of 48 different state laws that come into play. Many of them layer on HIPAA, so that comes into play, but just complying with the breach requirements of HIPAA is not enough to comply with all these state laws," Kottkamp says. "What ends up happening is that if you have pure PHI for HIPAA purposes, just health information and name, in almost all of those cases all of these state laws are not going to come into play because they are focused on financial information. However, in many situations where there is a breach of PHI, the contents of that PHI are broader than just pure health information. They might involve account information, or a deductible, or a credit card that was used to pay for that healthcare."

> "THERE IS A CRAZY QUILT OF 48 DIFFERENT STATE LAWS THAT COME INTO PLAY... JUST COMPLYING WITH THE BREACH REQUIREMENTS OF HIPAA IS NOT ENOUGH TO COMPLY WITH ALL THESE STATE LAWS."

The inclusion of any information like that most likely triggers state law requiring breach notification, he says. Then things get complicated. For instance, there are wide variations in state law and nuances about exactly how a breach notification letter must be worded.

"There are state requirements that you must send a letter to their respective attorney general or consumer affairs division prior to sending it out to those affected by the breach. There is a small number that require the state actually bless the letter before sending it to those people," he says. "Then there are the timing issues, and with HIPAA, 60 days is your outside limit. But 45 days in at least two states, and Florida has the current record for the tightest, which is 30 days. You can really get yourself tripped up if you are laser focused on HIPAA and send your notification letter, but if, for instance, you forget to send the required statement about putting a credit freeze on your account as is required in six states and given a nod in other states."

In addition to listing all sorts of universal contact information like the Federal Trade Commission and credit reporting agencies, Maryland and North Carolina require that the breach notification letter include state-specific information for contacting the attorneys general in those states.

"If you have a 50-state breach, you can't use the exact same breach letter for everyone affected by the breach unless you want to tell people in Idaho how to contact the

attorney general in North Carolina, which doesn't make much sense," he says. "People like to think they can use a broad notification letter that covers everything that any state could possibly require, but then lo and behold, they've missed something like that state-specific requirement."

Many states also have supplemental requirements within their state agencies, Kottkamp notes. Whereas most states require that you notify the attorney general, some also specifically require that you additionally and separately notify another agency such as the department of consumer affairs.

States also have different thresholds for when you must notify the attorney general and other departments in those cases. Some states require reporting only if the breach affects more than 500 people, Kottkamp notes, while others set the trigger at 750 or 1,000.

"If you have a multistate affair with more than just health information, you literally have to go state by state to make sure you're checking all the boxes," Kottkamp says. "Some smaller healthcare providers won't have to deal with a breach in multiple states, but larger health systems and other kinds of operations in the healthcare industry are going to find that a breach of any size is likely to involve people in more than just the one state where the company resides or is headquartered."

Even large organizations can overlook the risk related to state breach notification requirements, Kottkamp warns. A hospital or health system may have a solid plan for fulfilling HIPAA breach notification requirements but only address state requirements as an afterthought, assuming the federal compliance automatically satisfies the state or that state requirements are comparatively minor.

New York Goes After Delayed Notice

That is not at all reliable, and the consequences can be serious. States take their breach notification laws seriously, as evidenced by the New York attorney general's recent settlement with CoPilot Provider Support Services, Kottkamp says. CoPilot, which provides support services to the healthcare industry, waited more than a year to provide notice of a data breach that exposed 221,178 patient records.

The company blamed the delay on an ongoing investigation by the FBI, but agreed to pay $130,000 in penalties and to improve its notification and legal compliance program, the Department of Justice announced.

On Oct. 26, 2015, an unauthorized individual gained access to CoPilot's confidential patient reimbursement data via the website administration interface and downloaded reimbursement-related records for 221,178 patients. In mid-February 2016, the FBI opened an investigation at CoPilot's request, focusing on a former CoPilot employee. On Jan. 18, 2017, CoPilot began to provide formal notice to affected consumers in New York, more than one year after CoPilot learned of the breach of patient data.

"You're looking at audits and other sorts of regulatory actions by the states if you don't comply. If the state requires you to notify its attorney general and you don't, the state will see the breach when it comes up on the federal government's list of large breaches," Kottkamp says. "Then, they're going to contact you and ask why you didn't notify them. That's a big problem. That's an open invitation for the state attorney general to just come in and hammer that provider."

The most aggressive states are likely to be the ones with the toughest cyber laws, so the top of the list would include New York, Florida, California, Illinois, Ohio, and Massachusetts, Kottkamp says. Massachusetts also has an oddball statute that, unlike how almost every other state requires the provider to describe what happened in the breach, specifically prohibits the provider from describing the breach.

"I don't know if they're worried about copycats or what, but it's a bizarre law," he says. "That's a great example of how you might think you're doing the right thing because it's the obvious thing and what every other state requires, but you do that in Massachusetts and you're in trouble."

Any state with an outlier requirement — like Maryland and North Carolina with their requirement for notifying specific agencies, and Ohio with its 45-day time limit — are likely to be more aggressive about enforcement, Kottkamp says. They know those are unusual requirements and they will check to make sure you paid attention.

Risk managers and compliance officers should maintain a list of applicable breach notification laws for every state in which the organization does business, Kottkamp suggests. That may be a long list for many covered entities, even relatively small ones, he says.

"Whenever there is a breach and it's more than just pure PHI, one of the top five questions to ask is what states are affected," he says. "Then,

you pull the breach notification laws for those states and start layering. The sort of stained glass window you end up with dictates what you need to do for breach notification, and you may find that you have to write several letters and send to many different places by different deadlines."

One source for the state breach notification laws is a compilation by the National Conference of State Legislatures, which can be found online at: http://bit.ly/1ao7NAi. Several law firms also have compiled state-by-state guides, such as one by the firm Foley & Lardner, which is available online at: http://bit.ly/2vkPfzd. ■

SOURCE

- **Nathan A. Kottkamp**, JD, Partner, McGuireWoods, Richmond, VA. Telephone: (804) 775-1092. Email: nkottkamp@mcguirewoods.com.

New Breach Reporting Tool Helps With HIPAA Response

A new breach reporting tool should be useful for HIPAA compliance, partly because it can help providers stay on top of what is currently trending in cyberattacks and other types of breaches.

The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) recently launched the revised web tool, saying it puts important information into the hands of individuals, empowering them to better identify recent breaches of health information and to learn how the breaches are investigated and successfully resolved. The HIPAA Breach Reporting Tool (HBRT) features improved navigation for both those looking for information on breaches and ease of use for organizations reporting incidents.

The tool also educates on the types of breaches that are occurring, industrywide or within particular sectors, and how breaches are commonly resolved following investigations launched by OCR. The tool is available online at: http://bit.ly/1FrWfKp.

HHS Secretary **Tom Price**, MD, said HHS heard from the public that it needed to focus more on the most recent breaches and clarify when entities have taken action to resolve the issues that might have led to the breaches. "To that end, we have taken steps to make this website, which features only larger breaches, a more positive, relevant source of information for concerned consumers," he said.

HHS OCR originally released the HBRT in 2009, as required by the Health Information Technology for Economic and Clinical Health (HITECH) Act. It features public information that HIPAA covered entities report to OCR when they are involved in breaches of unsecured protected health information of 500 or more individuals. The tool includes the name of the entity, the state in which the entity is located, the number of individuals affected by the breach, the date of the breach, type of breach (such as a hacking/IT incident, theft, loss, unauthorized access/disclosure), and location of the breached information (such as a laptop, paper records, or desktop computer).

New features of the HBRT include enhanced functionality that highlights breaches currently under investigation and reported within the last 24 months; a new archive that includes all older breaches and information about how breaches were resolved; and improved navigation to additional breach information.

HHS said it plans to expand and improve the site over time to add functionality and features based on feedback.

HIPAA compliance leaders should find the improved tool useful, says **Jennifer R. Breuer**, JD, partner with the law firm Drinker Biddle in Chicago.

"OCR has always posted the wall of shame, the list of people with breaches — so it is the same tool we've had before, but more useful. The tool makes it easier to find the same information that was there before if you really took the time to dig through it," Breuer says. "You're able now to use the search capabilities and better understand why breaches have happened."

The most useful part of the tool might be the ability to monitor trends in HIPAA breaches, Breuer says. An individual case may not be so instructive, but a pattern could be, she says.

"It's not so important to know that hospital A did something silly and now they're publicly scolded, but it is important that you get a sense of how breaches are happening, the way in which your counterparts are falling prey to this problem that you're all trying to avoid," she says.

Seeing that one provider had trouble when an employee took a laptop home might not mean that

much, but if you see that several providers had breaches in the same way over a similar period of time, you might decide it is wise to take a look at your laptop policy, she says.

"You can see how people are actually accessing data inappropriately, and though some will be ways we all know about, some of the ways are evolving over time. You can get a better sense of the phishing and other attempts from external sources who are trying to access protected data," Breuer says. "You want to know what the risks are today, because they are changing over time."

Breuer's study of the data in the tool suggests there are plenty of the known human error-type breach causes, but there appear to be more phishing attempts and other outside attacks.

"It's a good reminder that both are still a threat and that you need to educate your people on the whole range of things that can result in data breaches," Breuer says. "There can be a tendency to think that this is a well-known issue among healthcare professionals and they know about all the standard ways you can have a data breach, so you only need to talk about cyberattacks. Or it can go the other way, but the truth is revealed when the data show that both still should be subject of your education efforts." ■

SOURCE

- **Jennifer R. Breuer**, JD, Partner, Drinker Biddle, Chicago. Telephone: (312) 569-1256.

Per-record Cost of Data Breaches Increasing

The cost of healthcare data breaches continue to remain the highest out of any industry, with an average cost of $380 per record, according to a recent report from the Ponemon Institute. Across all industries, the average cost for each lost or stolen record containing sensitive and confidential information decreased from $158 in 2016 to $141.

That means that a healthcare data breach costs 2.5 times more than the global average across other industries. The global average cost of a data breach is down 10% over previous years to $3.62 million. In the United States, the average cost for each lost or stolen record containing sensitive and confidential information across all industries increased from $221 to $225. The average total cost experienced by organizations over the past year increased from $7.01 million to $7.35 million.

However, companies are experiencing larger breaches. Globally, the average size of the data breaches increased 1.8% to more than 24,000 records, the report says. For all other industries, the average cost per record is $141.

The United States has a higher breach cost compared to Europe, which has shown a decline of 26% in cost year-to-year, with the difference attributed to the centralized regulatory environment in Europe. In the United States, organizations must adhere to federal and individual state regulations.

The report says the rise in breach cost also can be explained by the occurrence of HIPAA compliance violations and companies rushing to notify customers. The cost of issuing a notification of a breach alone is an average of $690,000 in the United States, which the report notes is twice that of any other country. The cost goes even higher when business associates are involved, increasing the cost by an additional $17 per record.

In the United States, Ponemon identified these factors that influence data breach costs: compliance failures, the extensive use of mobile platforms, chief privacy officer (CPO) appointment, and the use of security analytics. The use of security analytics reduced the per capita cost of data breach by $7.70 and the appointment of a CPO reduced the cost by $4.30.

"However, the extensive use of mobile platforms at the time of the breach increased the cost by $6.50, and compliance failures increased the per capita cost by $19.30," the report says. "Having an incident response plan and team in place, extensive use of encryption, employee training, BCM [business community management] involvement, and extensive use of data loss prevention technologies all reduce the cost of data breach by more than $9 per compromised record."

Data breaches due to third-party error, compliance failure, extensive migration to the cloud, rush to notify, and lost or stolen devices increased data breach costs by more than $10 per compromised record, Ponemon reports.

"To illustrate, a fully functional incident response team decreased the per capita cost of data breach from $225 to $199," the report says. "In contrast, third-party involvement in the breach incident increased the per capita cost from $225 to $249."

The full report is available online at: https://ibm.co/2rLVOKR. ■