HOSPITAL ACCESS MANAGEMENT™

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

INSIDE

RELIAS MEDIA

JUNE 2019 Vol. 38, No. 6; p. 41-48

In-Network Hospital Patients Still Receive Surprise Bills From Providers

A patient decides to undergo elective surgery. She acts responsibly by researching her coverage. After a few time-consuming calls, the patient is assured the hospital of choice is in-network.

Patient access staff play their parts, too. When the patient calls to schedule the surgery, they verify the insurance as in-network and carefully review the out-of-pocket costs with the patient.

Everything seems in order — yet weeks later, an unpleasant surprise bill arrives at the patient's house. It is not from the hospital, but from an out-of-network provider who was involved in the patient's care at some point during her hospital stay. The patient does not even recognize the physician's name. Not surprisingly, her first call is to the hospital to complain.

In one recent case involving this frustrating scenario, a patient underwent cardiothoracic surgery at The MetroHealth System in Cleveland. No one realized the surgeon was not in-network and was under contract with another facility. The patient received a bill on the other facility's letterhead.

The patient's daughter handed the mystery bill to **Kenneth W. Kirby,** CHAM, CHTS – TR, admitting manager. At first, it seemed something had been entered into the system incorrectly. Shortly afterward, Kirby spoke with a co-worker whose husband had received an out-of-network bill from the same surgeon. The true reason for the surprise bill became clear; it was much more complicated than just a system error. "I realized that the surgeon was not an employee of our hospital," Kirby says.

There are new data on just how often these surprise out-of-network bills are sent — about 14% of the time, on average.[1] "The topic of surprise billing has become increasingly important in today's healthcare climate," says study co-author **Jean Fuglesten Biniek**, PhD.

Surprise medical bills have been debated in state- and federal-level policy discussions, media reports on individual patient experiences, and recent academic literature. "The issue of receiving out-of-network care at an in-network facility has become particularly relevant," Fuglesten Biniek notes.

However, data on just how often this was happening were lacking. "We wanted to provide some numbers as to how prevalent this phenomenon is and

HOSPITAL ACCESS MANAGEMENT

Hospital Access Management (ISSN 1079-0365) is published monthly by Relias LLC, 1010 Sync St., Ste. 100, Morrisville, NC 27560-5468. Periodicals postage paid at Morrisville, NC, and additional mailing offices. POSTMASTER: Send address changes to *Hospital Access Management*, Relias LLC, 1010 Sync St., Ste. 100, Morrisville, NC 27560-5468.

GST Registration Number: R128870672.

SUBSCRIBER INFORMATION:
Customer Service: (800) 688-2421
customerservice@reliasmedia.com
ReliasMedia.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

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.

AUTHOR: Stacey Kusterbeck
EDITOR: Jonathan Springston
EDITOR: Jill Drachenberg
EDITORIAL GROUP MANAGER: Leslie Coplin

for which providers this is happening most frequently," Fuglesten Biniek explains. The researchers analyzed about 620,000 claims from 2016. All involved inpatients whose insurance was in-network with the hospital in 37 states and the District of Columbia. Some key findings:

- Overall, 14.5% of admissions had at least one out-of-network professional claim;
- States varied widely in the prevalence of out-of-network claims, ranging from 1.7% in Minnesota to 26.3% in Florida;
- The largest share of out-of-network claims (16.5%) came from anesthesiology;
- Of the in-network admissions with an independent lab claim, 22.1% of those lab claims were out of network;
- Emergency medicine accounted for 11% of the out-of-network claims.

"In one sense, the results were not particularly surprising," says **Bill Johnson**, PhD, another study co-author. Surprise anesthesiologist bills have received a fair amount of media attention.

"However, the fact that patients can go to an in-network admissions and receive out-of-network care is surprising, in and of itself," Johnson says. The sheer volume of the surprise bills also was unexpected. "Roughly one in seven in-network admissions had these associated out-of-network claims. This is a striking number," Johnson says.

Some out-of-network bills cannot be avoided by anyone in the revenue cycle since they involve physician groups external to the hospital. But in-network status with the hospital itself is a different story. Many problems can be avoided if patient access staff find it early. "From a revenue cycle perspective, communication is paramount when patients are having scheduled elective procedures out of network," Kirby offers. Patients need a full understanding of precisely what it means for them financially. "This would allow patients the opportunity to do some price shopping to see if they could come up with a better price," Kirby suggests. Arranging a discount is not out of the question. "Healthcare is competitive. Hospitals are strategically trying to attract new patients," Kirby says. While few consumers would pay sticker price for a new car, they do not realize healthcare costs are not always ironclad.

"If a patient is making a large bulk payment, they most certainly have leverage to negotiate," Kirby says. "Hospitals are very competitive when it comes to elective surgeries." MetroHealth's financial counselors give patients options before they receive services. Kirby suggests this scripting: *"Since you realize that you are out of network, and if you are in agreement with paying your out-of-pocket expenses upfront, we would like to offer you a discount of [blank]."*

Right when a patient is scheduled, preadmitted, or preregistered, patient access should jump on the opportunity to help the patient avoid surprise bills. "The front end should be trained to watch for out-of-network coverage and advise the patient accordingly," says **Pete Kraus**, CHAM, CPAR, FHAM, business analyst for revenue cycle operations at Emory Hospitals in Atlanta.

Still, surprise bills are tough to predict. "Where things get tricky is when physicians order consultations with out-of-network providers," says Kraus, noting that tests conducted by out-of-network labs also are problematic. "Tracking such contingencies mid-treatment is challenging. There are a lot of moving parts, so to speak."

The one thing patient access can always offer is education. "Staff can't

be experts on everything pertaining to patient third-party coverage. But they should be comfortable with general concepts," Kraus says.

Giving patients some specific questions to ask their health insurer is one way patient access can help. "To protect themselves from out-of-network expenses, patients must know enough about their coverage to ask questions of their providers," Kraus adds.

Of course, surprise bills can come up even with lab test results from providers the plan deems out of network. "It seems all but inevitable that the patient will blame the provider for arcane, hard-to-follow rules by a patient's insurer," Kraus says.

Savvy patient access staff can at least inform patients of this possibility in advance.

"This may help avoid a denial or reduction of reimbursement," Kraus offers. "But the provider will probably get blamed for the surprise bill anyway."

In dealing with patient complaints about surprise bills, scripting can help somewhat.

"It can assure a uniform response message. But by then it's too late," Kraus says. "The front-end proactive approach is essential. Preferably, this happens at the time of scheduling, but certainly when the encounter is preregistered and preauthorized." ■

REFERENCE

1. Kennedy K, Johnson W, Fuglesten Biniek J. Surprise out-of-network medical bills during in-network hospital admissions varied by state and medical specialty, 2016. Healthcare Cost Institute. Available at: http://bit.ly/2WlTwO0. Accessed May 3, 2019.

Must-Have Metrics to Track Productivity of Centralized Schedulers

Some patient access departments are moving toward centralized scheduling, where appointments are booked all in one place. There are many advantages to this; still, tracking productivity is a challenge.

"It is a very manual process. Many times, it does not paint the entire picture," says **Jessica Budri**, RN-MSN, APRN, senior manager in the patient access department at Connecticut Children's Medical Center. Centralized scheduling is fairly new at the health system; leaders implemented the system only within the past few years.

Important metrics include: How many calls are made? How many calls are received? How many patients are scheduled? How do incoming referrals compare to outward calls made to patients? These numbers are not readily available. "We do not have a reliable source of 'one-truth' data to gauge how the team is doing," Budri says.

Inaccurate data on productivity are an ongoing source of frustration. Phone reports give limited information on how many calls are made and how long each call lasts. "But we aren't consistently capturing those patients who cannot get through," Budri laments. Similarly, there are no good data on how many times staff try to contact one particular patient or family. How quickly the first incoming call from a referred patient is handled also remains a mystery. The number of appointments made by employees (the goal is at least 15 per day) is known, but the number of calls they answered is unknown.

"It is hard because it is phone tree-based, with little detail on a specific user," Budri notes.

The percentage of "dropped" calls (those that go to voicemail without anyone answering) are kept to an absolute minimum. "Our goal is to have zero dropped calls," Budri reports. "That is what we strive for but do not always achieve."

Many data points that would help the department assess its performance are not captured. "A key metric we would love to be able to [capture] is follow a referral through to completed appointment," Budri says. Other wished-for-but-elusive metrics: How much back-and-forth happens before registrars actually make contact with a family? And how long does it take from that point until an appointment is actually scheduled?

The quality of customer service given is hard to pinpoint, too. The Connecticut Children's Press Ganey surveys include two relevant questions about "the ease of scheduling" and "the helpfulness of the registration person." Schedulers receive a target goal and a stretch goal based on the previous year's results. "We are excited that we are currently above our stretch goal for both inpatient and outpatient registration services," Budri reports.

The medical center's social media specialist informs the department about when someone is posting about it. "This has helped us identify a few key opportunities very quickly," Budri says. One parent posted that they had called three times and still could not get through and hashtagged the facility. "This helped us quickly review the account, connect with the family, and provide service recovery," Budri says.

It turned out the parent had only called twice. Also, it had just happened the night before, allowing for a timely reply. "It still gave us great insight into a parent's point of view on the importance

of always being able to answer their calls as a free-standing children's facility," Budri explains.

Northwestern Medical Center in Saint Albans, VT, opened its Central Access Center in early 2019. Currently, the center is scheduling outpatient visits for eight of the hospital's 15 practices. "Our goal is to slowly incorporate all the practices over the next two years," says Patient Access Manager **Frederick J. O'Neill**. Staff also track referrals and obtain prior authorizations. "After opening the access center, it became evident that we needed to upgrade our phone system to one that provides more tools to measure productivity," O'Neill recalls.

Creating goals for employees was not the problem. "We had a 'magic number' of how many calls a scheduler can answer within an hour. That seems to be on track," O'Neill says. The department also measures the number of abandoned calls, which is at less than 1%. "But we currently have no way to monitor calls for quality assurance," O'Neill laments.

There also is no way to track appointments scheduled per employee. The department is working on upgrading its phone system. Also, patient access is working with electronic medical record vendors to add additional reporting features.

The new Central Access Center was implemented as "totally budget-neutral." O'Neill visited each practice to determine how many FTEs would be taken away. "We ended up using phone volumes to determine the amount of FTEs we would need," he says.

One hundred calls per day, on average, was considered equal to one FTE. For example, if an office answered 100 calls per day on average and had two FTEs working there, one employee was taken from that office. "It got kind of tricky with some of the smaller practices," O'Neill notes.

Next, each practice had to sign off on algorithms for how they wanted their patients scheduled.

"We had to standardize some of the scheduling processes across the practices," O'Neill says. It soon became apparent these were overly complex, with more than 60 different appointment types in the mix. "We wanted to reduce the amount so someone in the Central Access Center would not have to learn what each appointment code meant," O'Neill says.

Appointment types varied at all the practices and even sometimes differed for providers within the practices. Some were using a "consult" appointment type, while others used "new patient" or "office visit."

"In essence, they all meant the same exact thing," says O'Neill. "We worked with each practice to see if they could eliminate appointment types. We have been successful in a few areas." Many offices were fine with just using the "consult" type to simplify things. Patient access continues the work on reducing appointment types within the practices. "Some algorithms were updated five times in just the first few months of operations," O'Neill notes.

Inconsistent processes for patients who needed to follow up also were problematic. At some clinics, electronic triage messages were sent to nursing staff. Other practices transferred calls directly to a nurse triage line. "We were able to adjust staffing in clinics," O'Neill reports. "They now all have dedicated nurse triage lines." This important change makes things easier for schedulers, and patients appreciate it, too. "We have seen an increase in patient satisfaction," O'Neill adds. ■

New Possibilities With Preregistration If It Happens Earlier

Preregistration has been a hot topic at Baptist Health System in Birmingham, AL, for years, ever since the system transitioned to Epic in 2013. At that point, patient access leaders were discussing various opportunities for improvement across all facilities.

"Utilizing the new system, we had the ability to view more information," says **Wendy Lepp**, corporate director of patient access. This paved the way to expand preregistration.

Most importantly, CPT codes were attached to service descriptions in the new system. This gave patient access what they needed to follow up with physician offices and insurance carriers regarding the specific test performed. "Staff looked first at the cases added for the next day. Only when those were finished, did they look at cases further out," Lepp says.

Two years ago, patient access came up with the idea of preregistering the patient at the time they were scheduled. Early in 2019, the solution was implemented. The biggest worry was how execute the new procedure without adding any staff. In addition to their daily scheduling tasks, registrars also had to preregister patients who were scheduled for future dates.

"Our current process is to pull a schedule for tomorrow and preregister anyone who is still pending," Lepp says. When that schedule is completed, the staff move on to the next day, and so on. When the appointment is booked,

the account routes to a work queue, and a registrar contacts the patient. The new process was piloted at the smallest hospital in the health system first. "It has worked really well there," Lepp reports. "The staff have taken pride in making it work."

Next, it was brought to the second largest hospital in the system. Although the preregistration process is new, the department is already seeing benefits:

• **There are fewer complaints about surprise out-of-pocket costs.** "It's a patient satisfier," Lepp says. This is because many people are already worried about costs. Therefore, most appreciate getting some straight talk about what they're going to owe. If there are any issues, patients are connected with a financial counselor months, weeks, or several days in advance when there is plenty of time to come up with options.

• **Fewer procedures need to be rescheduled for financial or coverage reasons.** "We identify potential issues earlier, as opposed to just two days in advance," Lepp says.

Financial counselors and clinical staff in surgical departments work together to resolve insurance issues ahead of time. This means procedures can go as planned. For instance, a financial counselor might inform the clinical area that there is no precertification in place for a patient scheduled for surgery at 5:00 a.m., but that an approval is expected shortly. This allows the procedure to be moved to a different time but still proceed. The patient receives the needed care, does not receive a surprise bill due to a "no auth" denial, and the procedure does not have to be canceled.

• **Events progress smoothly on the date of service.** All preregistered patients are color-coded in the system (green if all they need to do is sign forms, purple if precertification is needed, and yellow if a copay needs to be collected).

In the past, staff looked first at cases added for the next day. Only when those were finished did they look at cases further out. "We are now starting when the patient actually gets scheduled," Lepp explains.

Cases are worked right away, regardless of whether the surgery or procedure is scheduled for the following day or months away. "Hopefully, everything will move out a little further," Lepp says. This gives everyone some wiggle room to address the inevitable problems that arise. Often, the problem is that the doctor's office never obtained precertification for the surgery. "If there's enough time to work with, it can hopefully be resolved without the need to reschedule," Lepp adds.

Although there are many benefits to preregistration, there also are some challenges. For instance, surprisingly often, people's insurance changes in some way after the initial preregistration call. "If you are working on a case this month, and it's scheduled for next month, things may change during that time," Lepp says.

Some patients have Medicare, but it is canceled by the time the procedure happens. Others have had Medicaid coverage, but it switches to an HMO. To catch these changes before claims are sent, a new process was needed. "We have a follow-up work queue that these accounts stay in until we can reverify the coverage during the month of the service," Lepp explains.

Another challenge is the sometimes-high costs for the patient, even with precertification in place.

"It comes as quite a shock. The concern then becomes: Is the procedure emergent, or can it be done later on?" Lepp says. Early discussions mitigate the stress for the patient, allowing for options such as payment plans to be considered.

Finally, even with enough staff to preregister scheduled patients, there are not always enough resources to follow up on all cases. "That's been our struggle," Lepp reports. "We finally got it worked out, I think." Previously, staff worked by service type; now, they work cases alphabetically. This distributes the workload more equally.

"It has also allowed staff to become more familiar with the insurance requirements for all services, as opposed to specific service types," Lepp says. ■

Millions More Are Insured, But Barriers to Care Persist

Thanks to the Affordable Care Act (ACA), millions more Americans are insured. However, that does not mean all these new customers can access healthcare without any trouble.

If someone bought an individual plan or if someone is on Medicaid, they encounter more barriers to care than those who are on employer-sponsored health insurance plans, according to the authors of a recent study.[1]

"The ACA introduced many policy changes that we didn't adequately understand the impact of at the time of our study," notes **Héctor E. Alcalá**, PhD, MPH, CPH, one of the study's authors.

In particular, the researchers wanted to know if lower Medicaid reimbursement rates would be associated with poor access to providers.

Further, Alcalá and colleagues set out to understand if the ACA insurance exchange offerings differed from other non-exchange insurance options in terms of access to healthcare.

"I was somewhat surprised that those with health insurance purchased through Covered California [that state's ACA exchange] had a harder time getting their insurance accepted by a primary care provider than those with insurance purchased [outside the] exchange," says Alcalá, an assistant professor in the department of family, population, and preventive medicine at Stony Brook (NY) University.

Researchers calculated the odds of being unable to access primary care doctors and specialists and schedule a needed appointment in a timely manner, using data from the 2014 and 2015 California Health Interview Survey. People on Medicaid or those who bought plans on the individual market struggled more in this area compared with people on employer-based coverage. Prior research has suggested there is no difference in the *quality* of care offered between exchange and off-exchange plans. However, no one had examined differences in *access* to care.

"Our study suggests that the barrier experienced by people purchasing their insurance coverage through Covered California is that primary care providers are less likely to accept their insurance, relative to other insurance coverage options," Alcalá says.

It is unclear what this finding means for hospitals. If Covered California options translate to poorer access to primary care, it may benefit hospitals and other practices to become part of the networks in Covered California. Currently, the Covered California networks are smaller than off-exchange networks. "This potentially leaves patients with fewer providers that are willing to take their insurance coverage," Alcalá says.

Hospitals can offer financial counseling to help people understand what all this means.

"But if providers are unwilling to take [patients'] health insurance coverage, this is unlikely to help those who are unable to pay for care out of pocket," Alcalá notes. ■

REFERENCE

1. Alcalá HE, Roby DH, Grande DT, et al. Insurance type and access to health care providers and appointments under the Affordable Care Act. *Med Care* 2018;56:186-192.

Do Not Leave Night Shift Registrars Leftover Pizza to Clean Up

Some night shift registrars face not only a crowded waiting room of patients upon arrival at work, but also a mess from the day shift's pizza party.

"Nothing can kill morale like coming in and finding all the leftovers that the day shift had — and you get to clean it up as well," says **Mike M. Harkins**.

For years, Harkins, now director of registration at Sentara Healthcare in Norfolk, VA, worked the night shift and found leftover pizza many times. However, Harkins' staff do not have to worry about this. "You must consciously have the same 'fun' for all shifts. It is only fair," Harkins says.

If the day shift eats pizza, fresh pizza is offered to evening and night shifts, too. "We order and pay for it in advance with places that are open late," Harkins explains. The same is true of communication. Day shifts sometimes gather in daily "huddles" to learn what is going on in the department. Meanwhile, night shift registrars have to settle for impersonal emails. Sentara Healthcare's registrars all receive information the same way regardless of what shift they work, whether it is in by email, bulletin boards, or in-person.

Another well-known morale-killer for the night shift: Staff meetings inflexibly held only on day shifts. Harkins makes sure meetings are held multiple times during the day. "Every employee has an equal chance to attend," Harkins notes.

Suddenly spotting a well-meaning but rarely-seen supervisor in the middle of the night has an unintended negative effect. "Employees become suspicious that you are checking up on them if you just show up randomly," Harkins says. Instead of surprise visits, all patient access supervisors put themselves on the schedule every other Thursday night. "This sends a consistent message to staff that they are in the building to work a normal shift," Harkins explains.

On alternate Thursdays, supervisors work a 7:00 p.m. to 7:00 a.m. shift. "They catch all three shifts, and it gives the supervisor off on Friday," Harkins says.

Employees who have small issues know that they can wait for the Thursday the supervisor is working to be heard. "People just want to vent sometimes, and we need to listen," Harkins says.

One supervisor recently noticed that computers and printers were not used because night shift registrars worked in a different location than the day shift.

New equipment was added in a more convenient spot. Another supervisor saw ED registrars constantly struggling with patient volume and added an additional registrar to the overloaded shift.

Even grabbing something to eat was once a problem; soda and chips in snack machines were the only option for off-shifts. "There was nowhere for the night shift to get a meal," Harkins says. To fix this, new snack machines were added, offering soups and sandwiches.

Savvy supervisors noted that day shift registrars tended to avoid restocking and cleaning.

"The attitude was, 'Leave it for the night shift, because they don't have enough to do,'" Harkins says. Supervisors made it clear that day shift registrars needed to do their part. On the other hand, supervisors also noticed some bad habits cropping up during late shifts, which were not scrutinized as closely. "Uniforms, food rules, and phone rules start to relax," Harkins notes. Requirements are reinforced consistently.

Most of the issues brought up by the night shift are no different than any other shift. "But if there is no avenue for night employees to be heard on a regular basis, things can grow out of proportion, causing bigger problems," Harkins cautions.

If morale is not the best, supervisors pick up on it before it gets out of hand. "Sometimes, it is great to bring in some ice cream and just spoil them a little bit," Harkins says.

Keeping up morale for night shift registrars is not an easy task. "We all know 24/7 operations can be a challenge," says **Pamela Konowall**, CHAM, assistant director of healthcare access at the Cooper Health System in Camden, NJ.

All levels of the patient access management team visit employees at all shifts consistently. Supervisors are scheduled for each shift, and monthly rounding is conducted with every employee. Konowall stays late or arrives early to hear what is going on during off-shifts. Recently, registrars complained that when they entered a patient's room to obtain demographic information, they would find out a colleague had already collected that information. It was frustrating both staff and patients, but a simple fix was found. "The resolution was to assign staff members to specific areas so it's clear which registrar is responsible for which room," Konowall says.

With supervisors physically present, off-shifts can let them know right away if scanners or computers are malfunctioning. If so, the equipment is immediately serviced and then tagged to indicate that it has been repaired.

Whenever managers reward staff in any way, they do not ignore the night shift. Recently, the ED registration team achieved a 20% increase in collections for the first quarter.

"All shifts played a part in meeting the goal, so all shifts were rewarded," Konowall reports.

Everyone earned a free takeout meal, which they ordered themselves from a restaurant of their choice.

"Third-shift employees have restrictions due to operational hours of fast food delivery options, but they do have a favorite food spot that delivers until 1:00 a.m.," Konowall notes.

Likewise, when personal notes written by supervisors are offered, managers make sure to do it for all shifts.

"One can see thank you cards proudly displayed by employees," Konowall says. ■

Avoid Over-Collecting From Patients: Refunds Mean Costs and Rework

Not collecting enough up front is an obvious problem. It leaves the patient with an unexpected bill. But collecting too much also is problematic.

"When a patient has to be refunded, this requires manpower and additional expenses for the revenue cycle," says **Ryan Mills**, MBA, director of access services for Baptist Health's East Region in Lexington, KY.

Refunds stem from too-high price estimates. Mostly, this happens because registrars use inaccurate benefit information to compute the patient's cost, but timing also is an issue. "The patient may have outstanding claims that process prior to the claim for the estimated service," Mills explains. If so, the remaining deductible, or the maximum out-of-pocket cost, ends up being much lower after those claims are processed. "This results in over-collection," Mills says.

Another scenario: The payer decreases the contractual allowance, but the estimator tool has not been updated to reflect this change. The result is the same: The patient pays too much.

When overpayments occur, the first step is to determine if the patient has any other outstanding balances. If so, the overpayment is applied to those accounts. Once all accounts are at a $0 balance, a check has to be mailed to the patient. This is a somewhat time-consuming process, Mills notes. Someone has to print the check, stuff it into an envelope, and run it through a

postage machine. "While it may add a few extra seconds to your registration times, the easiest way to prevent the need for refunds is updated benefit information," Mills offers. Sometimes, a second estimate, performed at the actual point of service, is surprisingly different from the first one.

"We have personally seen that estimates can drastically change based on benefit information in just a matter of a few days," Mills says. In one such case, a patient came to the ED a week before an echocardiogram. At the time of the echocardiogram, the claim for the ED visit had not been processed yet. The price estimate showed the patient owed $2,000 for the test. After the ED claim was processed, the true amount the patient owed for the echocardiogram turned out to be $900. The patient was refunded $1,100. "Even though we verified benefits at the time of service, there was no way to know how an unprocessed claim will be adjudicated," Mills says.

Timing is the single biggest cause of an estimate being too high, says **Jason Considine**, senior vice president and general manager of patient access, collections, and engagement for Experian Health. At issue is the time frame between creating a price estimate and when the insurance processes a claim. "As claims get processed, deductibles and maximum out-of-pocket amounts change," Considine explains.

An estimate may be created at a point when not one dollar of a $5,000 deductible has been met. By the time the actual claim for that visit gets to the insurance, other providers may have submitted claims totaling $5,000, thereby eliminating the deductible. "By the time the claim with the original estimate processes, there may be little to no patient liability left," Considine says.

Revenue cycle staff do not always have the right tools to give accurate price estimates. "Patient liability estimation is a complex process of calculating multiple components," says Considine, noting these include insurance benefits, charges, contractual adjustments, and provider discounts. "If hospital staff are manually estimating the processes, they could be using outdated pricing lists." These do not always factor in insurance benefits, contract rates, and discounts.

As a front-end leader, Considine directed staff to ask patients what they already paid toward their deductible in recent weeks.

"Without this check and the manual reduction of an estimate, you are almost guaranteed to over-collect," Considine says.

Baptist Health's patient access staff first submit an eligibility query. This tells them the patient's benefits. "For those payers who do not participate in automated responses, users can manually file the benefit into the estimator," Mills says.

Then, when the patient presents, registrars reverify eligibility and benefit information. This gives them a somewhat more accurate number. "It gets the most updated information from the payer," Mills says. "But we realize that unprocessed claims are not going to be reflected."

Services scheduled at the end of the year for a date of service the following year are particularly complex.

"Many times, we must wait until Jan. 1 to see the new plan year benefits," Mills says. Usually, the estimate is given at the time the service is scheduled. "But there are times that this is not feasible," Mills acknowledges.

Even if the service is weeks or months away, the cost estimate is performed anyway.

"But we inform the patient that a better estimate will be provided at the time of service due to possible changes in benefits," Mills adds. ■

HOSPITAL ACCESS MANAGEMENT™

HIPAA REGULATORY ALERT

CUTTING-EDGE INFORMATION ON PRIVACY REGULATIONS

Jussie Smollett Incident Shows Need for HIPAA Training, Audits

A Chicago hospital fired at least 50 employees for violating HIPAA by improperly accessing the medical records of actor Jussie Smollett, according to multiple news outlets.

The actor, known for his recent work on the television show "Empire," was treated there following an incident in which he claimed to have been attacked by two men outside his apartment in January. The case was the subject of extensive media attention and controversy because he claimed the attack was a hate crime. However, two friends told police that Smollett had hired them to fake the attack. The district attorney declined to press charges, a decision which was widely criticized.

Firing employees after improper snooping can be appropriate after the fact, but the better solution would be to stop the intrusions in the first place, says **Vish Davé**, senior associate of Schellman & Company, a global independent security and privacy compliance assessor based in Tampa, FL.

There are different steps that hospitals can take to prevent unwanted snooping by employees. One common method is to implement quarterly training and provide knowledge accessible to employees, including disciplinary action, when policies are not followed, Davé says. Furthermore, technical safeguards can be implemented within the electronic medical record (EMR), including access controls and audit controls.

"Access controls can be implemented so that they limit the amount of information an employee can access based on their authority levels and role type within the organization. For example, an employee working front desk who only needs to enter demographics or update demographics for patients might not need to access the patient's actual medical records and therefore will be assigned a role that prevents them from entering or accessing the medical records based on their role type," Davé explains.

Another technical safeguard, audit controls, provide healthcare organizations the ability to monitor access and activity within the EMR, including user login, logout, what health records are accessed, changed, and any irregularities found. They also provide organizations with audit trails that give them the ability to investigate any improper access, Davé notes.

Still another option available, depending on the type of EMR, can provide healthcare organizations the ability to mark certain patients' charts as confidential, Davé says. When an employee attempts to access the patient's chart, the system prompts the employee to give a justified reason of why the employee is accessing that specific patient's information and logs the reason into an audit trail.

"With the ever-changing technology environment, several other types of solutions are available within the market that work in similar fashions and detect improper access in near-real time based on the type of electronic healthcare record system to minimize employee snooping," Davé says.

Some EMR software offers role-based limitations granular enough that they limit particular categories of employees to certain fields in the EMR, notes **Kristen Rosati**, JD, an attorney with the law firm of Coppersmith Brockelman in Phoenix.

"For example, billing clerks may not need access to the entire EMR to do their job. However, not all EMR software has good technical role-based capabilities," Rosati says. "Even the best role-based limitations can't determine in advance whether a particular employee with treatment access has a treatment relationship with a particular

patient. It would have a very negative impact on patient care to require some type of prior association with the patient to allow access, because you have shift changes, doctors filling in for one another — many situations that would make that unworkable."

Hospitals have to rely on good advance training and after-the-fact auditing to confirm that employee access is appropriate. That makes it nearly impossible to prevent all infractions, Rosati says.

"Hospitals have training modules that explicitly tell employees not to peek at records out of curiosity. They explain how the audit trails will catch them, but they do it anyway," she says. "It comes down to people having shockingly bad judgment."

That was true back in days of paper medical records, too, but it was more difficult to gain access, Rosati notes. If someone famous was undergoing treatment, a nosy employee had to go where the record was stored and physically gain access to it. That was more difficult, but people were successful in their snooping, Rosati says.

"The good news is that in the electronic environment you know who accessed the record. With paper, you didn't," she says. "This problem of people peeking at records isn't new. It's just that we know how much it's happening now."

In the 23 years since HIPAA became law, Rosati says the incidence of snooping in patient records has decreased. She attributes this decline to healthcare employers educating employees about the consequences. "The vast majority of employees are very careful to follow these policies because they know what can happen to them," Rosati says. "There will always be some who can't resist."

Rosati notes that records snooping occurs with more than just celebrities. Access audits also should look for queries for patient records with the same last name as the employee, implying a familial relationship such as an employee seeking information to use against a spouse in a divorce proceeding. Audits also can look for unusual volume of access. If a billing employee typically accesses 50 records a day but then accesses 100 or 200, that could represent someone who is browsing records out of curiosity or to seek specific information for improper purposes.

Budgetary concerns can limit the security options for some healthcare organizations, notes **Brian McPherson**, JD, employment law and commercial litigation shareholder at Gunster in West Palm Beach, FL. Technology exists to limit employee access to records, but not everyone can afford it — especially if it means changing to a different EMR, he notes.

Another problem is that in many healthcare organizations, no one audits the logs showing who accessed patient files.

"HIPAA requires that hospitals and healthcare facilities have a medical record director who is charged with overseeing and auditing patient records. Records are kept of who accessed a record, when, and why," McPherson says. "The problem is that nobody goes back to see what the logs are reporting. The information is there but nobody is paying attention to it because they're so busy with everything else."

One tactic is to flag the records of known celebrity patients or others involved in newsworthy events such as crimes and disasters so that the system sends an alert to the medical record director when someone accesses those records. Also, the auditor can make a point of periodically reviewing the records of those patients for any access that seems unsubstantiated, McPherson says. Oversight like that may be how the Chicago hospital discovered the unauthorized access of Smollett's records.

Some hospitals also assign an alias to celebrity patients so that anyone looking for records under the patient's real name will come up emptyhanded, McPherson notes. Audits may reveal the unsuccessful searches, which still could result in disciplinary action.

"My experience has been that hospitals are not really on top of this until there has been a problem," McPherson says. "You have too many other things to spend time and money on. If your system seems to be working, nobody pays attention to this issue. But once they have a problem and it becomes public, then they're on top of it and implement more controls to protect those records."

On the other hand, some hospitals make a point of offering greater confidentiality for their patients, particularly facilities in communities with a higher percentage of celebrity patients. Sometimes, those hospitals market their enhanced record security to potential patients, McPherson notes.

The Smollett incident illustrates the limitations of simply telling employees not to look at celebrity files, says **Bill Joll**, head of worldwide sales for BlackRidge Technology, a technology security company based in Reno, NV.

"This case is consistent with other common HIPAA violations, where individuals either purposely or inadvertently access unauthorized medical records. It doesn't matter which, as the records are already compromised," Joll says. "Many healthcare organizations lack the

proper security and risk management solutions to prevent this. This is even more true within the broader med-tech solution and service provider ecosystem."

Joll notes that when HIPAA was put in place, organizations scrambled to implement policies and procedures to comply. They often took a simplistic approach to limiting access to patient records, he says.

"We've discovered over the years that many of the policies and procedures implemented stuck to the 'don't do this' or 'don't do that' level. Organizations generally put enough in place to pass HIPAA audits, but compliance with a particular statute does not equal security," Joll says. Many healthcare organizations correlate risk management to compliance. However, compliance audits are only a "point in time" snapshot of some auditor's perception of whether policies are in place and followed, Joll says. Audits do not give any visibility as to what is happening or enforced at every point in between, he says.

While security leaders in the healthcare industry are increasingly embracing a mix of security products to protect the organization, the technologies they deploy often are focused on post-breach detection, Joll says. "Compounding this problem, many hospitals lack the necessary resources to proactively review and monitor much of these solutions. Even if a detection product is in place, an attack or breach often goes unnoticed," he says. "This leaves many organizations in the position of having only policies and procedures in place to deal with [protected health information] and relying on adequate training of employees who are incentivized to focus on patient care rather than cybersecurity. Healthcare organizations must ensure that only authorized access of patient records is allowed by enforcing core internal security and access policies at all times, not just at the point of audit." ■

Microsoft Breach Reveals Risk From Cloud-Based Data Storage

A recent attack on email servers at Microsoft raises questions about the security of protected health information (PHI) on servers that healthcare organizations use.

On April 12, Microsoft sent notification emails to some Outlook account users warning them of a breach that might have compromised their data. Between Jan. 1, 2019, and March 29, 2019, hackers accessed a Microsoft support portal that is used to field customer questions and complaints. The hackers could have accessed and viewed the content of some Outlook accounts, Microsoft said.

"This unauthorized access could have allowed unauthorized parties to access and/or view information related to your email account (such as your email address, folder names, the subject lines of emails, and the names of other email addresses you communicate with), but not the content of any emails or attachments," according to the notice from Microsoft.

Later, Microsoft said the breach might have been worse than it first appeared and that accounts might have been accessed for months earlier than believed. The hackers might have been able to access email content and addresses, the company said.

Patients who may have shared PHI through these compromised accounts could be at risk, says **Mark Bower**, general manager and CEO of Egress Software in Boston. The administrative compromise of the Microsoft customer support portal allowed the attackers to gain full access to email content in compromised accounts as well as email addresses and subject lines, Bower explains. This could enable manipulation of the account owners network with well-constructed phishing emails for direct attacks and potentially more damaging access. "The attack illustrates that dependency on cloud email providers to protect data only means one thing for people: Attacks like this are to be expected, and getting ahead of the more serious risk of email data access requires trusted, third-party email encryption for sensitive emails with built-in smarts and monitoring so users are properly secured and warned when threats emerge," Bower says.

A primary lesson from the Microsoft breach is that anyone can fall victim to an attack, says **Matt Fisher**, JD, partner with Mirick O'Connell in Worcester, MA. Hosting your data with a massive company like Microsoft does not bring any guarantee of safety, he says.

"It's only a matter of when, not if, a breach will occur. Unfortunately, the hackers are steps ahead of people trying to protect the data. This incident shows that even a company as sophisticated as Microsoft is not beyond reach," Fisher says. Healthcare organizations using Microsoft email

servers should contact the company to determine if their data were involved in the breach. If it were, then try to determine if any PHI was compromised. If PHI was involved, one most likely will need to proceed with data breach notification, Fisher says.

Avoiding this type of breach in the future will require a review of security settings and optimizing them when possible, Fisher says. Sticking with the default security settings and options usually is insufficient. Generic passwords are especially vulnerable to outside attackers.

"It's possible sometimes when you look at your setup you will find that not all of the security features have been activated," Fisher notes. "After taking all the right steps up front, you have to constantly monitor and make sure systems are updated regularly. You also have to recognize when the threat environment is evolving and not remain static."

Fisher notes that the healthcare industry is known for its lack of vigilance on cybersecurity, although the level of attentiveness can vary greatly from one organization to another.

"It would be beneficial for most healthcare organizations to pay more attention to this and treat it with the utmost seriousness," Fisher says. "The Microsoft breach is a reminder that these attacks are continuing and can come from areas you hadn't anticipated."

For healthcare providers, this Microsoft email data breach brings to mind the healthcare data compromise in Singapore last year that affected 1.5 million patients and originated with an unpatched version Microsoft Outlook, says **Sam McLane**, chief of the technology services office at Arctic Wolf Networks, a software security company based in Sunnyvale, CA. The hackers in that 2018 case took advantage of a known vulnerability in Outlook, McLane says. The lesson for risk managers involved the need for good security hygiene, including regular vulnerability assessment and patching.

"The most recent Microsoft email episode involves Microsoft-managed email services such as Outlook.com, MSN.com, and Hotmail.com," McLane says. "It is important to note that this episode appears not to have affected Office365, which healthcare providers probably use for communications involving electronic protected health information."

For the healthcare community using Office365, a best practice is to monitor your Office365 login data for suspicious activity, McLane says. "Microsoft provides solid Office365 security and can provide tool security telemetry, but the burden lies with the healthcare organization to monitor Office365 telemetry for anomalous activity," he says. "Monitoring and detecting unauthorized access to Office365 like anomalous sign-in activity from brute-force attacks, concurrent access across multiple geographies, and access from unauthorized geographies are industry best practices that enable you to tighten up security of PHI in the cloud."

The latest Microsoft breach illustrates an important trend in cyber threats, says **Andy Smith**, vice president of product marketing at Centrify, a software security company based in Santa Clara, CA. "This breach is yet another example of the fact that cyberattackers don't hack in anymore. They login using weak, default, or otherwise compromised credentials," Smith says. "Privileged account access provides cyber adversaries with the keys to the kingdom and a perfect camouflage for their data exfiltration efforts." A report from FireEye, a security company based in Milpitas, CA, indicates that the global median dwell time that attackers remain undiscovered in your network is 101 days (as of 2017). Healthcare organizations have to assume that bad actors are in their networks already, Smith says. That is why healthcare organizations must move toward a "zero trust" model of cybersecurity. "Zero trust" is a security concept in which organizations do not trust anything inside or outside its perimeters. Anyone and anything must be verified before granting access.

"Simple static passwords are not enough, especially for sensitive company data. Now is the time for healthcare organizations to move to a zero trust approach, powered by additional security measures such as multifactor authentication, to stay ahead of the security curve," Smith says. "With static passwords, how are you supposed to know if the user accessing data is the valid user or just someone who bought a compromised password from the 21 million that were revealed in the 'Collection #1' breach? You cannot. You can't trust a static password anymore; multifactor authorization is the lowest hanging fruit for protecting against compromised credentials."

Smith says healthcare organizations must take a stronger stance against hackers because the evidence is clear that they are not letting up on trying to get access to valuable PHI and the associated data of patients.

"Zero trust can help companies avoid becoming the next breach headline, including the damage to brand, customer loss, and value degradation that typically comes with it," he says. ■