HOSPITAL ACCESS MANAGEMENT™

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

INSIDE

Sharply reduce number of questions patients must answer. 67

Good responses to complaints about patient identification. 68

Eliminate the toughest obstacles to correct price estimates. 69

A simple form helps those who arrive without an appointment 70

Staffing techniques to meet the needs of walk-in patients. 70

Tailor financial conversations to patient's situation 71

Signs that registrars live up to patient expectations. 71

HIPAA Regulatory Alert: Vendor security compliance; beware social engineering scams

RELIAS MEDIA

SEPTEMBER 2019 Vol. 38, No. 9; p. 65-72

Authorization Process Slower Than Ever: Some Payers Take 2 Weeks to Give Answer

Anyone who finds out he or she needs a diagnostic test urgently already has a lot on their mind. The last thing they are probably thinking about is how long it will take for their insurance plan to decide if it is even going to cover the test.

"For nonurgent services such as diagnostic scans, the auth review could take up to 15 days," says **Junko I. Fowles**, CHAM, supervisor of patient access and financial counseling at the Huntsman Cancer Institute in Salt Lake City, noting that the preauthorization team makes same-day and next-day add-ons a top priority. "If it's an urgent add-on and gets denied due to no auth, we'll appeal the denial." If the appeal is unsuccessful, the patient typically is not billed.

Payers are not all the same when it comes to time frames. Major payers (who use third-party utilization management administrators) usually take two or three business days, according to Fowles. In contrast, some Medicaid and Medicare Advantage HMOs take double or triple that time.

Staff has found it helps to mark some services "urgent." These are usually radiology add-ons as well as surgery and inpatient admission. "The insurance utilization management team expedites the review of these cases," Fowles explains.

Cases of patients with chronic illness (such as heart disease, cancer, or transplants) are not usually held up. That is because these cases are reviewed by case managers, who already are familiar with the patient's situation. "As soon as they review the most recent clinicals, preauth can be approved within 24 hours of the submission," Fowles says.

Sometimes, no authorization is required — at least according to the payer rep. The problem is that another entity is really the one making the decision. It turns out that a separate company handles authorization requests for the payer.

"Later, the claim is denied because the third-party authorization company was not contacted," says **Karan Levering**, CHFP, assistant vice president of preaccess services at Mariottsville, MD-based Bon Secours Mercy Health.

Average turnaround time for authorizations is somewhere around a

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

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

week, but some payers take twice that long — not a day sooner than their contracts allow for. "Several payers, including medical mutual and our managed Medicaid plans, typically utilize the entire 14-day time frame," Levering reports.

To try to get an answer on what is taking so long, revenue cycle employees sometimes spend 45 minutes on a single call. They are forced to work their way through an automated phone tree before they can talk to a person. "The phone system at many payers is cumbersome and complicated," Levering says.

Patient access leaders offer these techniques to help speed and simplify the authorization process:

• **Examine problematic payer contracts.** "It is important to review and understand contract terms. Often, these may allow for long response times," Levering says. If contracts allow payers to take up to four weeks, they probably will. Patient access employees are not directly involved in payer contracts, but they still can do something about the issue. "Leaders can enlist the help of the hospital's managed care department if there are issues with authorizations," Levering suggests.

To add to the misery, payers sometimes take even longer than their contract allows. "Though not the norm, this can create additional challenges," Levering adds.

• **Use automated technology to verify authorization status.** "This is one of the most beneficial improvements we have seen," Levering notes. Tools can tell registrars if an authorization is needed. It also indicates the status of authorizations daily, eliminating cumbersome manual checks.

"This has greatly increased productivity for our preaccess teams," Levering reports. If a valid authorization is on file with the payer, it is removed from the worklist automatically. If no authorization is in place, the tool prompts the associate to follow up.

Some payers post authorization requirements online; however, this often does not occur at the CPT code level, according to Levering. Not all payers accept electronic requests for authorizations. Those that do vary greatly on how they want it submitted. "This takes additional resources and time to complete," Levering says.

• **Streamline the peer-to-peer review process.** Payers are requiring many more peer-to-peer reviews, with the patient's physician and the insurance company's physician reviewer discussing the case on a call. "It is challenging for physicians to find time during their day to stop and complete these," Levering observes.

• **Assign patient access employees to obtain authorizations.** Like most health systems, Paterson, NJ-based St. Joseph's Health is seeing a huge increase in authorization requirements.

"The HMOs have increased the amount of CPTs that will require authorizations by 25%. This seems to change constantly — without any real reason for the change," says Patient Access Manager **Samirah A. Merritt**, DBA, MBA. Payer time frames have grown longer (up to two weeks).

A typical scenario: A patient receives a prescription for a diagnostic test. The registrar contacts the physician's office that sent the patient for the test to let them know the patient came for testing. At that point, the office should request authorization from the insurance company. They do not always do so.

The next day, the registrar checks the status. Sometimes, nothing at all has happened to secure authorization.

"It can take up to a week to return the information. In some cases, the 48-hour window has closed," Merritt says.

The provider has that much time to request an authorization after the service is ordered. After the time is up, the payer will not give the authorization. Ultimately, the claim is denied only due to the timing of the request.

If the cutoff is approaching, registrars do what they can to speed things up. If all else fails, Merritt calls the office manager directly to explain the urgency of things. "To help combat this issue, we have assigned two people to the high-dollar modalities," says Merritt, who notes these employees normally handle outpatient registration. "On their downtime, they use the previsit workflow to ensure we obtain the auth prior to the patient's arrival."

The department has found some success in this approach, but it comes at a cost to productivity. Staff are spending much more time reaching out to doctors' offices.

"In some cases, we are following up all the way until the patient goes up for their procedure," Merritt reports. ■

'I Already Answered That Question': A Valid Complaint About Repeating Information

A comment such as *"I already answered that question"* once was common at WellSpan Health in York, PA. These days, a comment like that is rare thanks to some recent changes in the preregistration process designed to stop redundant questions.

"It's one of the things we all need to do better," says **Tracey Shetter**, CHAM, manager of the organization's patient access call centers.

Like most people, Shetter has been frustrated hearing redundant questions at many healthcare appointments. At a recent appointment, the registrar asked for an insurance card, even though it had just been verified at the lab in the same health system.

"We have an EMR system for a purpose. Staff need to be actually looking at it," Shetter says. Redundant questions, a well-known source of dissatisfaction, was a topic at some recent meetings. "It is an objective we are going to start to work on as an organization," Shetter reports.

At the call center, employees routinely asked for all demographic and insurance information. They did so even if the system indicated someone else collected this information already. Some patients complained, and such redundancies wasted employees' time. Still, it was not easy to teach staff to stop asking the questions.

"It is a cultural change. It's getting everyone to see that this is the purpose of Epic, and that [repeat questions are] driving our patients crazy," Shetter says.

Staff could see if the information was verified already; the problem was that staff did not trust the process was handled correctly. "It's a matter of trusting that whoever clicked the 'verify' button really did what they were supposed to do," Shetter explains.

Also, this problem was not isolated to the call center. Needless questions were asked in radiology, doctors' offices — anywhere patients presented. Shetter decided to make her department an example of how to change this long-standing practice. She told her staff, *"Trust has got to start somewhere, and it's going to start with us."*

It took multiple discussions over a period, but call center employees changed their ways. Now, they ask for information only when they have to. However, the same was not true of other hospital areas. Some people are preregistered by the patient access call center; such patients assume they will not have to answer more questions.

But when they present for services, registrars at those sites repeat questions anyway, according to Shetter. Confused patients complained they had given all the information over the phone already.

To prevent this, Shetter reached out to leaders. She encouraged them to educate registrars on how to tell if the patient had been registered already. If that is the case, and the patient already has an account number, there is "absolutely no need to ask the same questions over again," Shetter notes.

All call center interactions are recorded for quality assurance. "The big thing is making sure our personalities on the telephone are what they should be. It's all in your voice," Shetter explains.

In addition to a friendly tone of voice and other criteria, QA specialists listen for redundant questions. If they are repeating questions, employees are coached not to do so in the future. On the other hand, staff are responsible for

making sure information is up to date, including emergency contacts. Now, once somebody hits the "verify" button, it is valid for 60 days. There are three possible scenarios:

• **It is more than 60 days since the patient last presented.** This means a full preregistration is needed, but staff do not just fire away with a long list of questions.

They start with a matter-of-fact explanation: *"I see it's been longer than 60 days since we last verified your information, so I will need to go through that again."*

With this kind of intro, says Shetter, "people answer far more willingly. The conversation goes more smoothly."

• **The call center does not need to contact the patient at all since all the information was verified sometime in the past 60 days.** If the patient was seen at a doctor's office recently and insurance was verified there, staff just complete the registration from the work queue. "We then don't even need to call the patient," Shetter adds.

• **A full preregistration is not needed, but some information is missing.** Usually, it is answers to the Medicare Secondary Payer questions that are missing. Staff begin the conversation by explaining that Medicare requires them to carry out this step every time for all Medicare patients.

Other times, the patient is coming for a diagnostic test that could be accident-related. This would not apply for services such as mammograms that clearly are unrelated to accidents. The question does need to be answered for most other tests, such as CT scans.

"If it turns out the test is being done due to an accident, it changes what insurance should be billed," Shetter explains. For this reason, staff really need the information before the claim is sent out.

Ideally, the question is covered at the point of scheduling, but it does not always happen.

"We reminded the schedulers to ask this question. If the answer is 'no,' we won't have to call the patient," Shetter says.

If this piece of information is missing, call center staff need to contact the patient. They explain, *"I see that you recently verified your information at another WellSpan location. I just have a few questions related to this visit."*

Now that call center staff have stopped asking redundant questions, productivity has spiked. This is due to decreased call volume.

"We are seeing an average of 1,500 fewer calls each month," Shetter reports. Calls are answered in less than 30 seconds, on average.

Patient satisfaction is better because people can talk to someone immediately. "Nobody likes to sit on hold," Shetter observes. "We are only calling the people that we really need to talk to."

Shetter says the next challenge is to teach other registration areas to stop asking questions mindlessly. More patients are registering online now through the health system's patient portal. Too often, when these patients arrive for an appointment, all the same questions are asked again.

"Staff are so much in the habit of asking all the questions," Shetter says. "They are just trying to do their job well. It was always something you just did." ■

When Patients Are Identified Multiple Times for Their Own Safety

In clinical areas, asking for information multiple times can annoy patients. "We frequently get asked questions like, *'Why can't you retain this information for the future?'* or *'Don't your computer systems talk to one another?'"* says **Catherine Shull Fernald**, DNP, RN, RNC-OB, NEA-BC, chief nursing officer for acute care at Christiana Care Health System in Newark, DE.

Unlike in registration areas, where redundant questions are asked often, the queries are intentional. Their purpose is to prevent patient safety disasters, such as giving medication or performing a test or procedure on the wrong patient.

In clinical encounters, patient identity needs to be verified repeatedly for safety. "Along any process, there could be a misstep, which could lead to unwanted consequences," Fernald notes.

A label might be misplaced while someone is donating blood. Or, a donor might have fainted, causing a disruption with increased risk of an error. "By asking the donor name and date of birth at every step in the process, even if the technician is the same person throughout, it reduces and potentially eliminates any chance of error," Fernald explains.

Registrars ask for people's name, spelling, address, date of birth, and insurance information — often more than once. They do apologize, but at the same time they explain why.

"I am sorry for the inconvenience. We ask multiple times to verify your information as a way to ensure your safety at every step in the process of caring for you. By asking each time, we ensure it is the most current information, and we are able to prevent or correct any mistakes."

Registrars respond "patiently and respectfully," Fernald says. "Our patients have the right to understand what we're doing and why." ■

Patient Access Fine-Tunes Price Estimate Process

At Indiana University Health in Indianapolis, a cost estimator team works tirelessly to give patients good information on what their care will cost. "The estimate is tailored to a patient's care plan," says **David Burton**, vice president of revenue management.

The team of nurses and experienced billing and collections staff sort through all the facts that are known at the time. Despite their best efforts, the patient sometimes owes more than anyone anticipated. The devil is in the details.

"Changes in the details can impact the cost to a patient," Burton explains. Certain issues affect what is billed:

- The location where services will be rendered;
- The physician who will provide the services;
- The billing methodology for that location and physician.

A dermatologist might be able to perform minor surgical procedures in his office, but more complex services are performed in the hospital's OR. "Insurance companies may pay both the hospital and the provider differently based on the location," Burton notes.

To avoid pitfalls, staff must be familiar with the patient's insurance coverage and benefits. Understanding benefit accruals also is important since some patients pay a deductible in addition to co-insurance. Correct estimates are only possible if one knows how much of the deductible has been met already.

Some people have met their out-of-pocket maximums already. In that case, there are no co-insurance or other out-of-pocket costs to pay. "Each patient's circumstances are unique. It's based on specifics of their benefit plan and how much care they have received to date," Burton explains.

The team accurately translates the planned services into billing codes. Lastly, they need to accurately apply a patient's health insurance plan to all of the above. "A change to any of these factors can result in a different estimate amount," Burton says.

The team retrieves its information from multiple sources. "We often talk to the patient and their provider, or the provider's team," Burton says.

Even if someone receives the same service as another patient, both with the exact same insurance, they can end up owing different amounts. "Each patient's needs are unique. Their estimate must be customized to meet those needs," Burton explains.

One patient might need a longer hospital stay than the average person. Other times, patients end up consuming different or additional services. Things do not always go as planned. For example, a patient with COPD who is undergoing a routine hip replacement might need extensive postoperative respiratory therapy. That patient is going to stay in the hospital later. "These nuances can lead to varying out-of-pocket responsibilities," Burton observes.

Even with meticulous planning, estimates are off sometimes because something changes along the way. Other times, the patient buys a new insurance plan with completely different coverage.

To add to the complexity, payers might provide their own estimates to patients, which can be faulty. One reason is that the payer estimates do not factor in all the relevant information. The estimates usually are based on average costs rather than specific details of a patient's care.

"These may be incomplete or inaccurate. It causes confusion," Burton says. Staff make it clear to patients that the hospital's estimates can be trusted because they factor in all the available information. In contrast, says Burton, "payer estimates are often based on claim history. That can be very different from a patient's exact circumstances."

The department's price estimate process has expanded greatly in recent years. "We started small in 2015," Burton notes. At that time, staff prepared price estimates only for outpatient radiology services, and at just one location. The department now performs estimates for all locations as well as inpatient and outpatient areas (which includes laboratory services).

"Additionally, we have implemented a formal quality assurance program and retroactive audits," Burton reports. These show that 90% of estimates are accurate within 5% of the patient's actual billed.

Another recent change: Patients can request estimates online anytime.

About 8% do so currently. "These are processed like any other request, though they tend to require a bit more research," Burton says.

Ninety-five percent of estimates are completed within 24 hours; 85% are handled the same day. If the process takes a little longer, it is usually because staff need to follow up with physicians to confirm the details. Complex cases also take more time.

At Albany (NY) Medical Center, enrollment specialists are the ones who provide price estimates to patients. They are clear that actual charges may differ from what is quoted. "One issue we can face sometimes is the physician office not respecting the process," says **Brenda Pascarella**, CHAM, associate director of patient access.

There are times when offices schedule elective services before staff can give a price estimate to the patient. "Patients need to be made aware of the potential out-of-pocket costs," Pascarella says. ■

Outpatient Clinics Seeing Many More Walk-In Patients

Registrars at Tampa, FL-based Moffitt Cancer Center have seen a surge in walk-in patients at outpatient clinics for some time. "[There was] such an increase that we put a team together to handle this situation," says **Marion Knott**, manager of clinic access.

Clinics see anywhere from one to eight patients a day who simply show up. A few clinic managers, the outpatient nursing director, and Knott created a standardized process to meet their needs.

Often, patients came to outpatient clinics asking to see a clinician right away, but no one was available immediately. Registrars were put in the position of asking these patients to wait without knowing their needs. The team took two steps:

• **They defined the term "walk-in."** This term meant different things to different people. It was defined as any patient presenting to the clinic without a scheduled appointment at that particular clinic. "This distinction was important, because many people have multiple appointments on the same day at different clinics," Knott notes.

• **They created a "walk-in form" for all outpatient clinics to use if someone arrives without an appointment.** Patients indicate on a checklist the reason for their visit. The completed form is handed to the patient access rep, who determines the next step.

"It really depends what the patient is there for," Knott says. If they are dropping off documents or want a prescription refilled, staff encourage them not to wait. However, if they are in need of medical attention, the nurse is paged right away.

If the nurse does not respond within 15 minutes, the rep pages the clinic operations manager for assistance.

"For all other nonurgent requests, we ask if the patient would like to wait," Knott says. Staff note on the form whether the patient is going to wait and give the form to the nurse to assess. On certain occasions, the nurse determines that the patient really needs to schedule a visit with the provider. "If so, they work with the patient access representative to get the patient registered," Knott reports.

Staff also record the time each walk-in patient presents and what time the nurse sees patient.

"The clinic leadership is responsible for each of their staff's follow-up accuracy and timeliness," Knott reports. ■

Two Big Obstacles to Success With Walk-Ins

Walk-in volumes are surging, according to **Laura Marston**, a principal in the Chicago office of ECG Management Consultants.

This is especially true in primary care and pediatrics. It also is happening for any services that people can shop around for, especially imaging. For the revenue cycle, these are the two biggest challenges, according to Marston, who specializes in revenue cycle and access operations:

• **It is difficult to staff properly with unpredictable volumes.** The best approach is to trend typical walk-in volumes by day and time. "These data can then be used to build appropriate capacity into physician schedules," Marston explains. If walk-in volume is very high, additional registrars might be needed. "Registration kiosks can also expedite this process," Marston adds.

• **There is a chance the payer will deny the claim.** Insurance verification can be conducted in seconds, right when the patient presents. If authorization is not required, the process is straightforward. As long as the insurance checks out and copays are paid, the patient is seen right away. However, if an authorization is needed, things become far more complicated. Clinical information is needed, and the referring provider has to handle his or her part.

"Coordinating with the payer can take some time," Marston says. To reduce financial risk, "there are a few critical factors," Marston notes. Registrars need good training on how to verify insurance, collect from the patient, and choose the correct plan in the system.

"As many payers as possible should be integrated into a real-time eligibility tool," Marston offers. ■

Propensity to Pay Tool Gives Best Possible Options for Patient

A small but growing number of hospitals run "propensity to pay" tools on patients. This tells facilities how likely people are to need a payment plan, charity care, or financial assistance.

"Propensity to pay analytical tools are used to tailor payment plans, loan qualifications, needs-based discounting, and charity determinations," says **Jonathan Wiik**, principal of healthcare strategy at TransUnion Healthcare.

Ideally, the tool is used before patients arrive for all scheduled visits and for all walk-in patients before they are discharged, Wiik says. Only about 10% of hospitals do so currently. About one-third of hospitals give price estimates before service.

"If the patient is unable to pay, analytics are performed to determine the financial position of the patient," Wiik explains.

The propensity to pay tool is used to make decisions on down payments, payment plans, loan qualifications, needs-based discounting, and charity determinations. All this varies, says Wiik, depending on the urgency of the clinical intervention and the financial position of the patient. The best-case scenario: That it is all figured out during a preservice phone call. This is especially important for self-pay patients and those with high balances.

"Most hospitals' yield in this area for financial clearance of all patients is in the 50-60% range and can be as high as 80-90% on the scheduled patients," Wiik reports. Registrars at Intermountain Healthcare in Salt Lake City now calculate a propensity to pay score.

"This helps guide ongoing conversations with the patient," says **Todd Craghead**, vice president of finance and the revenue cycle.

The score determines the next step revenue cycle staff will take. Certain patients clearly qualify for some sort of financial assistance, so staff can help them apply for it. Others need guidance on how to set up payment plans.

Patients who require a financial conversation are grouped together. Patients who need to set up payment plans are handled separately. "Accounts are flagged based on the results," Craghead adds. ■

It Is All About Service: Use Data to Measure Progress

Customer service in revenue cycle areas is quite challenging for many reasons.

The revenue cycle role "mixes financial components into the clinical experience," says **Melissa Patten**, associate vice president of patient access at Northern Light Health in Brewer, ME. "There are sensitive conversations happening during times of illness and injury," adds Patten. Registrars are usually the first (and last) with whom patients interact. Wait times, cleanliness, billing process, and clinical care all factor into how satisfied someone is with the hospital.

"All of these integrate with the revenue cycle, often behind the scenes," Patten notes.

Many persistent dissatisfiers are out of the revenue cycle's control, including rescheduled procedures due to inclement weather, wait times due to emergency situations, changes to applications that happen as part of a system implementation, and staff who duplicate efforts while going through training. This is why knowing where the department stands

is so important. "Having consistent customer service expectations for staff is important," Patten says.

She carefully tracks certain data to gauge how the department is performing, including wait times (both call center and on-site), eligibility and coverage discovery, claims denials, no-show rates, accuracy of price estimates, and staff productivity.

"These metrics help leadership hold staff accountable," Patten says. "Both clinical and financial processes factor into overall satisfaction."

For surveys to be of any use, patients need to complete them timely. These surveys also require "pointed questions with specific answers to extract appropriate information," Patten underlines.

Rounding in registration areas is a way to obtain better feedback from patients. "Patient experience coordinators can spot-check progress and assist with escalations," Patten says.

When patients give positive feedback about their registration experience, it is shared immediately. "This helps to connect revenue cycle staff who may be removed from direct patient interaction," Patten adds.

How registrars treat patients and family directly affects the hospital's bottom line, says **Michelle Fox**, DBA, MHA, CHAM: "Consumerism has hit the healthcare industry, and it is here to stay."

Revenue cycle employees must be held accountable for providing exceptional service.

"How we treat our customers has a direct impact on our business," says Fox, director of revenue operations/ patient access at Health First in Rockledge, FL.

At Health First, all job descriptions include a "Customer Experience" section under the primary accountabilities. Registration counselors are expected to:

- Greet others with a smile, pleasant tone, and good eye contact;
- Be approachable and accessible when others need assistance;
- Deliver patient and registration paperwork to the patient care areas timely;
- Maintain successful relations with other patient business services, Health First associates, and physician office staff;
- Provide exceptional customer service to every patient, every time.

"The challenge with customer service is that it is not easy to measure," Fox says, noting that not all patients take time to complete surveys. "It's also hard to pinpoint exactly where the improvement opportunities exist due to the questions being asked."

Also, only patients receive the surveys; family members do not. "Not all customers are patients. How do you measure their satisfaction?" Fox asks. "You can only do so much with the information you have."

Despite these challenges, revenue cycle departments must find ways to be more "customer-centric," Fox says. "This needs to be communicated to every associate." ■

COMING IN FUTURE MONTHS

- New efforts to stop balance billing
- Patient access leaders join hospital committees
- Payers steer patients to outside locations
- Free morale-boosters for registrars

HOSPITAL ACCESS MANAGEMENT™

HIPAA REGULATORY ALERT

CUTTING-EDGE INFORMATION ON PRIVACY REGULATIONS

Vendors Continue to Be Weak Point in HIPAA Security

Vendors always have been one of the most worrisome parts of HIPAA security because hospitals and health systems must rely on them for the appropriate technological and physical security for protected data — without the ability to dictate exactly how.

Research shows that those fears are well founded, with many health organizations experiencing an increase in investigations and fines from HHS that are related to poor vendor HIPAA security. A study from the Ponemon Institute, a research organization in Traverse City, MI, that addresses data protection and information security practices, found that health systems are increasingly worried about their reliance on third-party medical devices and how they could compromise protected health information (PHI).

Seventy-two percent of respondents said they believe the increasing reliance on third-party medical devices connected to the internet is risky; 68% expressed similar concerns about connecting medical devices to the cloud.

Risk management processes are not keeping pace with cyber threats and vulnerabilities, according to two-thirds of those surveyed. Sixty-three percent also said their security efforts cannot keep pace with the growing use of digital applications and devices. *(The report is available online at: https://bit.ly/2SCDSg4.)*

One of the more interesting findings was that 56% of respondents had experienced a third-party data breach in the past two years, says **Ed Gaudet**, CEO of Censinet, a company based in Boston that provides risk management software for healthcare organizations. Earlier research had suggested lower rates of third-party vendor breaches. "It's kind of amazing that there is all of this money going into healthcare data security; yet, the data breaches are still trending upward. If you just look at this year alone, in the first half of the year we've already had breaches affecting more records than in all of last year," Gaudet says. "We think the attack surface, the cumulative measure of the points where someone can try to gain access, is actually getting bigger, not smaller."

In years past, the attack surface was on software and hardware that you controlled in your data center, Gaudet explains. That has changed dramatically in recent years, he says.

"Now, it's the Wild West. So much of your business processes are being outsourced and your data is hosted in the cloud. It is a completely different attack surface from just five years ago," Gaudet says. "We think the problem is going to get bigger. The risk analysts are woefully unprepared for this because a lot of their risk processes are manual or ad hoc, taking a lot of time."

Assessments Seen as Costly

At the same time, healthcare organizations are feeling the need to draw skilled digital security professionals to other pressing needs rather than have them spend so much time on verifying vendor security, Gaudet says.

A troubling finding in the Ponemon report was that 76% of healthcare organizations see their vendor risk assessments as costly, inefficient, and having no effect on reducing exposure to a breach, says **Larry Ponemon**, PhD, chairman and founder of the Ponemon Institute. He also was concerned to see that a majority of respondents thought senior executives in their organizations were allowed to skip the vendor risk

assessment when they wanted to secure a lucrative business deal.

Ponemon also notes that 54% of respondents said they were at risk of a data breach because they could not complete a risk assessment of all vendors.

That shortcoming may be even worse than it appears because those in charge of HIPAA security may not even know all the vendors who potentially can access PHI.

"Healthcare is so complex that there can be an enormous number of vendors and third parties involved. In some cases, their access to secure data is not so obvious. If you don't know they even have that access, you don't put them in the process for risk assessment," Ponemon says. "Organizations are not doing all they can do create a safe and secure environment for protected data. A portion of that is due to the organizational culture that does not make this a priority."

There also is a significant budget gap to address, Gaudet says. The survey respondents said they need 2.5 times their current budget to adequately address the data security threats from third-party vendors.

Little Confidence in Effectiveness

Gaudet also calls attention to how many study participants assessed the effectiveness of their vendor security procedures. There was a big disconnect between how important they consider those procedures and how effective they think they actually are.

"We asked about the importance of data breach response procedures, and everyone said they were very important, but they didn't consider their own response procedures very effective," Gaudet explains. "The same result came from things like prior authorization of vendor risk, with a great majority saying it was very important, but only 36% of them saying they are doing it effectively."

Ponemon suggests that risk managers and other healthcare leaders use the data to push for more resources and a better buy-in from upper management when discussing the need for data security.

Gaudet agrees, saying the data give risk analysts and IT professionals the information they need to make the business case for a more robust vendor risk assessment program, which may include upgrades in staffing and technology.

Cloud apps and connected devices have increased the risk of data breaches sharply, leaving some IT professionals and HIPAA compliance leaders feeling unable to keep up, Gaudet says.

"Cloud apps have been expected, but the connected devices have surged quickly with more and more consumer-connected devices and the internet of things. When you combine that with the increased attacks and vulnerability, you have a perfect storm of factors coming together for professionals responsible for protecting organizations from a data breach," Gaudet says. "That is what is what is driving a lot of the pressure and anxiety in healthcare organizations." ■

Checklist Items for Selecting a Compliant Vendor

There is no quick and easy way to select a vendor to trust with HIPAA-sensitive data. It requires some legwork to determine what kind of security they have in place and possibly identify any shortcomings.

Organizations using hybrid systems (where some data are hosted in the cloud and some within the organization on a server) open more avenues for data breaches due to the complexities of the system's landscape, says **Sunil Konda**, vice president of product at SYNERGEN Health, a company in Dallas that provides software and consulting services for healthcare organizations. So far in 2019, 79 healthcare privacy incidents have been reported, including at companies such as OXO, BlackRock, Ascension, Rubrik, Advent Health, UConn Health, EmCare, and Quest Diagnostics, Konda notes.

"Pre-emptive and proactive cybersecurity crisis plans are important. As the use of digital healthcare services such as telemedicine, electronic health records, and wearables become the new normal in the industry, there has been an increase of cybersecurity threats due to the growing number of points of entry for hackers looking to capitalize on highly sensitive and valuable information," Konda says. "The question isn't if but when there will be a breach, as there is a high chance that every organization across industries and sectors will encounter some level of cyberattack at some point."

To reduce the chances of a security breach, Konda says there are eight essential items that healthcare entities should look for when selecting a vendor to meet the challenges of keeping patient information safe:

• **Information Security, Quality, and Compliance Framework.** A cybersecurity compliance framework

provides steps and recommendations on implementing and managing various aspects of the vendor relationship. Putting committees in place with coordinators ready to address compliance, information security, and quality and knowledge management creates a strong approach that spans the width of the organization to show how trustworthy the vendor is, Konda says.

• **Policies and Attestations.** When entering into an agreement, the policies and attestation standards should be clearly developed and presented. Key areas include HIPAA compliance audits, quality policy, and information security policy.

• **Administrative Safeguards.** Administrative policies and procedures should be in place to address security with agreements, business associates, and supplier management. Periodic audits of processes, documentation, and compliance protocol along with annual assets, risk assessments, and technical compliance reviews will further strengthen a vendor's security measures, Konda says.

• **Physical Security.** Ensuring the server room is monitored and nonessential areas are restricted to unauthorized employees or guest access will assist with physical barriers. Additional physical security measures include 24/7 closed-circuit television monitoring and biometric access control.

• **Technical Infrastructure Security (Cybersecurity).** The investment of a cyber infrastructure with multiple levels of security will assist vendors in preventing external and internal threats. Using encryption, secure backups, and additional network security, hackers' attempts to gain access can be prevented.

In addition, vendors need to show proof that a third-party organization is contracted to conduct penetration tests on the network on an annual basis to identify any vulnerabilities, Konda says. Proper action then can be taken to correct any detected risks.

• **Human Resource Security.** Steps vendors can take to mitigate internal personnel security risks include a robust screening and background check prior to the applicant's employment, continuously updating access control during employment, changing of roles within the company, and proper termination procedures to safeguard access throughout an employee's tenure with a company, Konda says. Scheduling monthly and quarterly reviews and compliance refreshers can assist with creating a company culture rooted in security and compliance.

• **Incidence Response.** The vendor should have a comprehensive incident response framework in place in case of a breach. Konda says this framework should be made up of essential personnel including but not limited to an interactive response technology team lead, an IT expert, legal representative, and management. It also should include steps to review and assess the incident and impact of the breach on the business, the response, implementing temporary and permanent fixes, and reporting to law enforcement officials.

• **Applicable regulations.** Ensure vendors are up to date with major U.S. laws and regulations. This includes the Health Information Technology for Economic and Clinical Health Act Omnibus Rule, HIPAA, and the Fair Debt Collection Practices Act. ■

Social Engineering Scams, Attacks Can Threaten HIPAA Security

Despite years of educating healthcare staff about the need for data security and the myriad ways people can worm their way into an otherwise secure system, employees still can fall prey to social engineering scams and allow HIPAA data breaches.

Social engineering refers to the ways hackers and other criminals prey on people's natural tendencies and weaknesses to create a way into a data system. It remains a huge problem, says **Dan Hanson**, an insurance and risk management professional with Marsh & McLennan Agency in Minneapolis.

"The problems caused by social engineering have been with us for a long time now. Bad actors use a variety of schemes to hack into business databases, pose as qualified vendors — often referred to as reverse social engineering — or even gain access to physical spaces," Hanson says. "There are literally thousands of variations. The only limit to the number of ways hackers can socially engineer users is the criminal's imagination."

Social engineering plays a role in most HIPAA breaches. Clinical Pathology Laboratories in Texas recently reported that PHI of approximately 2.2 million patients had been compromised in the data breach at American Medical Collection Agency (AMCA), which provides debt collection services to healthcare organizations. *(Read more at: http://bit.ly/2YvtCrg.)* AMCA reported that a cyberattack on its

payment website allowed hackers to obtain PHI for eight months. AMCA filed for bankruptcy after the attack. *(Read more about the filing at: https://bloom.bg/2GB8ARS.)*

A healthcare organization can even experience multiple forms of exploits in a single attack, Hanson says. These are some of the most popular forms of social engineering:

• **Phishing.** The most common scheme, often using fear and threats to create a sense of urgency, all in an attempt to wrangle usable information.

• **Pretexting.** Usually a fabricated scenario designed to fool an employee to extract information.

• **Baiting.** Similar to phishing but often promises a reward to entice victims, such as free music or movie downloads, to steal login credentials.

• **Quid Pro Quo.** These attacks promise a benefit in exchange for information, usually some kind of a service (e.g., an offer of IT that promises a software update but is instead a way to install malware).

• **Tailgating.** This involves someone without proper authentication literally following an employee into a restricted area.

• **Identity Theft.** The hacker steals an employee's identity he or she can use online or even create fake ID badges to gain access to the office.

Many companies know about these schemes and they have often made attempts at guarding against them. But the unfortunate truth is the criminals have become smarter, and they are constantly changing and updating their schemes, Hanson says.

"Just because many social engineering scams, like the Nigerian prince, seem so obviously fake and illicit, you can't assume that all schemes will be equally obvious to your employees," Hanson says. "Hackers are uniquely adept at spotting the flaws in their attacks and revising them. A lot of these people are incredibly smart and very good at what they do."

One of the latest innovations is invoice manipulation. This form of attack is not necessarily new but it has received more notoriety lately because it has become a bigger problem than ever before, Hanson says. Criminals posing as suppliers, vendors, or even customers attempt to defraud a company using fake, duplicate, or inflated invoices. It is important for companies to be vigilant about checking every invoice, Hanson offers.

Invoice manipulation has become a go-to attack choice for bad actors hacking email accounts, intranet, or databases. Hanson describes one way it can work: An employee's email is hacked, or their credentials are stolen. Now, the hacker has access and can monitor emails to determine who sends or requests an invoice. The hacker knows the company's vendors and sends an invoice that appears to be legitimate, but the routing, account, or vendor ID numbers have been altered.

"Guard against invoice manipulation by empowering employees to double check any time anything changes — numbers, banks, addresses," Hanson says. "Have them call the vendor directly to ask whether or not the information is legitimate. Don't send emails. If the hacker is already in your system, it's easy to fake the response."

If the hacker has no luck gaining access digitally, he or she can coerce or even hire a disgruntled employee. This is potentially the most powerful attack because the employee has physical access to the organization and generally can move anywhere without any restriction as well as access company data, Hanson says.

"A lot of companies are still getting caught flat-footed. It's not hyperbole to state that all organizations are, at one time or another, getting hit by social engineering attacks," he says. "All it takes is one employee to not be thinking clearly. That's when bad decisions are made. That's why continuous training is necessary."

Hackers who engage in social engineering attacks prey off human psychology and curiosity to compromise their targets' information, Hanson notes. Guarding against most of these does not require much more than paying attention to the details. But it is important to keep reminding employees how they can avoid social engineering schemes. Hanson suggests frequent reminders on these safeguards:

• Do not open emails from untrusted sources;

• If offers seem too good to be true, they probably are;

• Lock laptops;

• Read and know the company privacy policy;

• Do not react too quickly — hackers want someone to act first and think later;

• Be suspicious of unsolicited messages;

• Beware every download;

• Foreign offers are fake — end of story;

• Delete any request for financial information or passwords;

• Reject requests for help or offers of help;

• Set spam filters to high;

• Do not be afraid to ask questions or delay decisions until thoroughly checking out the situation. ■