FOR MORE THAN 30 YEARS

HOSPITAL ACCESS MANAGEMENT™

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

INSIDE

RELIAS MEDIA

SEPTEMBER 2018 Vol. 37, No. 9; p. 81-88

Big Expectations for 'Transparent' Costs: Can Patient Access Meet Them?

Calls for healthcare transparency are growing louder. Smart patient access departments are heeding those calls.

"The hope is that making healthcare prices known will lead patients and their advocates to shop for care based on price," says **Anna D. Sinaiko**, PhD, an assistant professor of health economics and policy at Harvard T.H. Chan School of Public Health in Boston.

Several states have passed laws requiring that hospitals provide price quotes on request. Generic information isn't enough; it must be personalized according to the patient's insurance.

"The federal government, along with individual senators and representatives, is also calling for greater transparency," Sinaiko says. There is increasing evidence that prices vary widely for the same medical services, even within local areas.[1,2] However, studies show only limited correlation between clinician prices and quality. "Expensive care is not, on average, better quality," Sinaiko notes.

Requiring hospitals to post charges is of surprisingly limited benefit to patients. "It is an imprecise way to help a patient plan financially," says **Suzanne Delbanco**, PhD, executive director of Berkeley, CA-based Catalyst for Payment Reform.

Posted charges represent little more than a hospital's starting point for negotiation with health insurers. "Almost no one ever pays the 'charge' amount," Delbanco explains. Insurance plans negotiate steep discounts. Patients usually only pay their deductible, copay, or coinsurance. Therefore, says Delbanco, "health insurers are likely in a better position to give patients more precise out-of-pocket estimates."

Patients want to know what they are in store for clinically. Wary of skyrocketing healthcare costs, patients also expect to understand what they are facing financially. "Increasingly, they want to know this upfront, before the services are rendered," says **Michael Thompson**, president and CEO of the Washington, DC-based National Alliance of Healthcare Purchaser Coalitions.

Often, patient access staff cannot provide a good answer for patients. One reason is lack of information on how contracts are structured for each payer. "The hospital payments are only the tip of the iceberg," Thompson offers. Multiple professional services and other services also are added to the patient's bill. Bundled

HOSPITAL ACCESS MANAGEMENT

Hospital Access Management™ (ISSN 1079-0365) is published 12 times annually by
Relias LLC
111 Corning Road, Suite 250
Cary, NC 27518-9238

Periodicals Postage Paid at Cary, NC, and additional mailing offices.

POSTMASTER: Send all address changes to:
Hospital Access Management, Relias LLC
111 Corning Road, Suite 250
Cary, NC 27518-9238

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

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

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

AUTHOR: Stacey Kusterbeck
EDITOR: Jonathan Springston
EDITOR: Jill Drachenberg
EDITORIAL GROUP MANAGER: Terrey L. Hatcher

payments are a growing trend, to promote transparency on how patients and plans are billed for procedures. "Expect to see more of this going forward," Thompson adds.

A new proposed rule from the Centers for Medicare & Medicaid Services (CMS) mirrors other earlier price transparency efforts. The agency is focused on requiring charges to be published online so those charges are publicly available to patients.[3]

"While this is admittedly a first step for CMS, publishing charges has shown little practical utility for patients in previous efforts nationwide to improve price transparency," says **Samantha Wyld**, a senior director at Optum Advisory Services.

Patients may not be interested in receiving an answer to a general question like, *"What is your standard charge for this procedure?"*

"This often has no correlation to the patient's out-of-pocket obligation," Wyld argues. Patients want an answer to a different question, one that is more difficult to answer: "What is this going to cost *me*?"

"Price transparency legislation is not new," Wyld notes. "In fact, 'early adopter' states like Massachusetts have been passing price transparency legislation since 2012."

It is no longer enough for hospitals simply to meet the specific requirements of the CMS proposed rule. "Organizations need to go above and beyond legal requirements to truly take the mystery and ambiguity out of healthcare costs," Wyld offers.

Patients want nothing less than customized price estimates from patient access departments. "It's critical to get this right," Wyld stresses. These take into account each patient's unique insurance coverage, plan benefits, contract structure, deductibles, and coinsurances/copayments. Sinaiko sees the movement toward price transparency as a "work in progress." One thing is certain: Patient access must develop better processes for generating insurer-specific price estimates. "Efforts will focus on making patients aware that they can shop for healthcare based on price, and to make price information more readily available," Sinaiko says.

According to Wyld, patients are not just going to the closest hospital anymore. People make healthcare choices based on out-of-pocket obligations, how easy it is to obtain that information, and the convenience and flexibility of payment options to meet their financial obligations.

"Hospitals win or lose patient loyalty based on whether they can provide a premier and differentiated experience," Wyld says. This is true both for price-shopping patients and for patients already receiving services at the hospital, she says. Wyld says patient access departments should take these steps:

- **Engage in financial discussions earlier.** "Patients want and need to anticipate their out-of-pocket costs before receiving care, way before receiving a bill, to be prepared financially for their share," Wyld says.
- **Ensure that staff are capable of conversations about out-of-pocket costs.** "Leaders should be ensuring they have the right skill development and education for staff in patient-facing roles," Wyld advises.
- **Measure performance when it comes to price estimates.** "Leaders need to gauge how their organization stacks up in terms of delivering a strong and seamless patient financial experience," Wyld adds. ■

REFERENCES

1. Newman D, Parente ST, Barrette E, Kennedy K. Prices for common medical services vary substantially among the commercially insured.

Health Aff (Millwood) 2016;35: 923-927.
2. Hussey PS, Wertheimer S, Mehrotra A. The association between health care quality and cost: A systematic review. *Ann Intern Med* 2013;158: 27-34.
3. *Federal Register*. A proposed rule by the Centers for Medicare & Medicaid Services, May 7, 2018. Available at: https://bit.ly/2wxb6WQ. Accessed Aug. 2, 2018.

Patients Want Self-service Estimates and Exact Dollar Amounts

Price transparency and price estimates have been two critical focus areas for El Camino Hospital's financial services team for more than two decades.

"Since 1996, we have offered cost estimates to any patient or prospective patient who called our office requesting one," says **Karla Romero**, manager of patient access at the 420-bed hospital in Mountain View, CA. "We have experienced a steady increase in the number of patients and prospective patients wanting to know what their out-of-pocket cost will be."

This is because of the surge in high-deductible plans. "Consumers want to be able to make informed financial decisions about where they go for care," Romero explains. Patients must plan for their medical expenses in advance of a procedure or hospital stay. Many callers reported searching in vain online for price information. "We wanted to find a solution that would allow patients to run their own personalized cost estimate," Romero reports.

The department's online price estimator tool launched in August 2017. It allows both current and prospective patients to instantly run an estimate based on their insurance benefits, the hospital's charge master, and contractual agreements with payers. The tool offers estimates for 90 services and procedures and 11 surgeries. For more complex surgeries, patients work with a financial counselor to learn their out-of-pocket costs.

"Since we launched the online self-service option, there have been more than 3,000 queries run using the tool," reports **Terri Manifesto**, senior director of El Camino's revenue cycle. Patients expect more than just a rough idea of their charges. "They want to know the exact amount of their future bill," Romero stresses.

Patient access has to explain their limitations in this regard. Only an estimate, based on the information available at the time, is possible. Once patients see a dollar amount, many ask another question, Romero says: "We're seeing an increase in people asking for additional discounts."

Many hospitals still offer only an average cost for a particular service, but Manifesto says El Camino's estimates "are between 95% to 99% accurate."

Still, employees caution that things can change.

"The final cost will be different if the deductible status or insurance changes, or if services ordered by the patient's doctor differ," Manifesto cautions. ■

Quality Assurance Dashboard Spotlights Issues

Manual processes are no longer enough to conduct the kind of quality assurance (QA) patient access leaders need at Winston-Salem, NC-based Novant Health.

A team of 15 representatives handles QA duties. "But as good as they are in their work, it is not enough to really give us what we want," says **Craig Pergrem**, senior director of preservice and onsite access for Novant.

Patient access is a multifaceted division in the revenue cycle. "QA can be challenging due to all of the different touch points patient access has," says **Elkin Pinamonti**, MHA, assistant director of onsite access for Novant Health's greater Winston-Salem and northern Virginia markets.

Many people in the patient access department view a patient's account before it even gets billed out. "This means that multiple team members have ownership of the account," Pinamonti notes. With any QA system, there's always the possibility that data can get "muddled and skewed," Pinamonti says. For instance, some team members may be included in a QA audit, even though their function with the account was very minimal. "Therefore, they would need to be excluded from the audit. Depending on your system, this delineation can be very difficult," Pinamonti explains.

The QA team examines about 10% of monthly volume. "When we went live with Epic, we determined that it would provide us with the data we

needed. We cancelled our QA vendor," Pergrem says. Soon, patient access leaders encountered a problem. "We could not maintain the same level of clean data with just work queues," Pergrem says.

Now, Novant's Epic revenue cycle team is attempting something new. "We are creating a QA process within the system by bringing work queues and other reports together on a dashboard," Pergrem reports. This information goes directly to team members.

The department's analyst, who is a former patient access manager, created the new QA dashboard. "It is like a reboot to QA for us. Each individual can see where they are having issues," Pergrem explains.

The department always watched closely for errors. The problem was that the information did not always make its way to the person who made the mistake. The dashboard allows leader to put patient access processes under the microscope.

"We want to see what patient access causes when it comes to a bill dropping or not," Pergrem says. Patient access staff are more aware of how their role affects the "big picture" of the revenue cycle.

"We will then build those key items into the scoring," Pergrem says. "It has been a process, but we feel we are getting closer." Accounts randomly sampled for monthly audits give only limited information. "It will not give your team members or your leaders specific data drilled down to individuals," Pinamonti says. The best QA system "needs to start at the end user level and it needs be in real-time," Pinamonti offers. The goal is for registrars to readily access information to address issues head on.

"Although monthly QA can be helpful in identifying departmental trends, it doesn't dig deep enough into what our individual team members may be missing on a day-to-day basis," Pinamonti says.

Novant wants to give employees a QA system they can use throughout their day. If an employee makes an error, he or she finds out so it can be fixed. Employees also receive an overall accuracy score. Pinamonti expects to see "big improvements" from the new QA system. "It is vital to set expectations for what a team member's role will be in the QA process, or it will lose its value." Employees are expected to ensure their accounts are error-free before they move to the billing phase of the revenue cycle. "We are continuing to see an increase in the importance of front-end registration's role in the billing cycle," Pinamonti notes.

Most employees really want to know how they can improve. "One of the biggest benefits of a great QA process is that it allows them to take control of their day-to-day work," Pinamonti says.

Employees identify their own needs for training, instead of leadership telling employees. "Delivering cleaner, more accurate QA allows for more trust in the system," Pinamonti says. "This increases utilization and buy-in."

The new ability to fix errors in real time positively affects revenue in three key ways, according to Pinamonti.

"It allows for registrations to be cleaner, decreases rebilling of accounts, and ultimately assists with your overall A/R." ■

Is Patient's Complaint Exaggerated? Recordings Tell the Real Story

Are patient access staff explaining consent forms accurately to patients? Are they interpreting and explaining insurance benefits correctly? Face-to-face recordings of registrations let patient access leaders at CHRISTUS Trinity Mother Frances Health System know these things for certain. "We listen to a sample size of recordings from random associates each month and report out on the findings," says **Tim Holland**, MPA, CHAM, regional director of admission services. Here are two lessons the department learned from the recordings:

• **Staff were entering information into certain data fields inconsistently.** This was mostly happening when patients refused to give their email address, or did not have one to provide. Some employees entered a generic fake email address (such as "noemail@noemail.com") into the data field. Others typed in a note about the patient's refusal to provide an email contact.

"We even found some cases where an associate thought they were using a 'generic' format, but it turned out to be an actual email address," Holland reports. This was corrected immediately because of concerns about patient privacy regulations, in the event the email was used to communicate with the patient about upcoming appointments.

• **Staff were not explaining consent forms to patients consistently.** "This was extremely concerning for us," Holland says. Leaders took immediate corrective action to ensure staff were relaying information appropriately. "Our forms have a lot of information on them," Holland notes. "We require our team

members to explain the 'high points' of the form before the patient signs."

For example, the hospital's consent form contains five boxes that a patient initials:

- Consent for treatment;
- Photography consent for clinical use;
- Authorization for release and/or acquisition of information. This refers to releasing or obtaining protected health information (PHI) to or from third parties to adequately provide care;
- Consent for electronic sharing. "We share PHI with other Epic facilities electronically when one of our patients utilizes another health system," Holland explains;
- HIPAA's privacy notice. Instead of waiting for inevitable questions from patients, employees anticipate them. Not surprisingly, most concerns involve "authorizing the release of information."

"We pre-emptively explain this point to patients to improve our efficiency," Holland adds. Occasionally, the recordings reveal that some additional education is needed. "Where we run into trouble is when an associate says that the patient is giving us the right to release information as we please," Holland reports. This incorrect statement would rightfully cause a patient to become concerned. Staff were reminded that the information is released only when requested or warranted.

Some associates offered no explanation at all about the consent forms; they simply asked the patient to, "please initial here."

These issues arise from time to time. Interactive videos are used to help associates understand the forms better. "We provide multiple education opportunities to make sure we are covering the legal forms correctly with our patients," Holland says.

Occasionally, a patient accuses someone in the department of acting overly aggressive with collecting. Sometimes, the complaint is about rude treatment. In the past, this was a "he said/she said" situation, but it is no longer a mystery for leadership. "We now use the recordings to either validate or disprove the patient's complaint," Holland says.

Most of the time, it turns out that the employee was not really at fault. One patient claimed they were "badgered" for money. In reality, the patient was politely asked for payment a single time. When the patient stated that they could not pay, the conversation moved on, and registration was completed.

On the other hand, collection practices sometimes really go too far. In these cases, appropriate action is taken. "But overall, the recording tool is not used as a 'Big Brother' approach to managing our teams," Holland notes.

The emphasis is on providing the best possible service for patients. Employees also realize they are protected from unfounded complaints. "The program has been very well-received by the majority of the team members," Holland says. "We consider it to be a huge win for the department." ■

Auth Already in Place as Payer Requires? Claim Still Might Be Denied

Patient access diligently obtains a required authorization from the payer and the service is scheduled. Weeks later, the claim is denied. However, it is not for "no auth," but because the payer says it was not medically necessary.

"Some payers actually issue an authorization, but once claims are received, they are denying for medical necessity," says **Maria Lopes-Tyburczy**, CHFP, director of patient access at Hackensack Meridian Health Palisades Medical Center in North Bergen, NJ. Mostly, this happens with inpatient admissions. Payers either downgrade the patient status to observation, or deny the entire claim. The claims always are appealed. "But we have very little success overturning the payer's initial decision," Lopes-Tyburczy laments.

There are two ways patient access is tackling this costly problem:

- **Staff identify when a payer consistently denies claims for medical necessity, even when the authorization was in place.** Patient access contacts the payer's representative assigned to the hospital. "Conference calls are scheduled to review claims and come to a resolution," Lopes-Tyburczy explains.
- **Staff are careful to meet all payer requirements.** For outpatient scheduled ancillary services and same-day surgeries, patient access verifies coverage and benefits beforehand. This ensures that the procedure is covered under the patient's policy, avoiding a "noncovered service" denial.

"Patient access works very closely with the referring physician's office," Lopes-Tyburczy says. All clinical information required by the

payer is sent in a timely manner. If preauthorization requirements are not met the day before a scheduled procedure, both the patient and the physician are notified. The procedure is canceled and rescheduled. Constant communication with payers and physicians is needed to avoid problems.

"Patient access is very diligent in ensuring that all information is obtained prior to date of service," Lopes-Tyburczy reports.

Obtaining authorizations for scheduled services is difficult enough. If time frames are shorter, it is even more challenging. "The struggle comes when physicians send patients for stat procedures," Lopes-Tyburczy notes.

When this happens, patient access employees:

- obtain the preauthorization requirements from the payer after verifying coverage and benefits;
- contact the referring physician's office, tell that office to follow up with the payer, and obtain a case number.

Sometimes, the referring physician calls the payer and conducts a peer-to-peer review with the payer's physician. Hopefully, this results in authorization. "If the payer states that the case is still in review, the stat procedure is done," Lopes-Tyburczy says. "Patient access follows up the next day."

Payers are constantly changing their medical necessity criteria. This further complicates matters. "Patient access staff training is ongoing," Lopes-Tyburczy says.

For walk-in patients, the medical necessity check occurs at time of registration. If medical necessity criteria are not met, the physician's office is contacted. "In some cases, patient access [staff] obtain additional diagnosis codes that are documented in the patient's chart," Lopes-Tyburczy says.

If no additional information is obtained, or if patient access cannot reach the physician's office, an Advance Beneficiary Notice (ABN) is issued to the patient.

"The patient can opt to have the procedure done and be financially responsible if Medicare denies the procedure," Lopes-Tyburczy says. The patient also can opt not to decline the procedure. Either way, patient access notifies the physician and ancillary department of the decision.

"A copy of the ABN is given to the patient. We scan a copy into the EMR for future reference," Lopes-Tyburczy adds.

This comes in handy if the patient ends up undergoing the procedure later. The registration system automatically alerts the patient accounting system that the patient accepted financial responsibility if Medicare denies the claim.

For all Medicare beneficiaries, a medical necessity check is performed using the information the physician's office provided. For scheduled ancillary services, a different process is used. At the point of scheduling, ancillary departments request that the physician send an order with the required information. This allows patient access to conduct the medical necessity check before the date of service.

"This gives us enough time to reach out to physicians' offices for additional diagnosis codes if needed," Lopes-Tyburczy says. ■

The Virtues of Real-time Registrar Observation

Patient access leaders can learn a lot from annual evaluations or soliciting feedback at staff meetings. But, sometimes, they learn even more from observing an employee during a shift.

Thirty minutes each day, usually between 9 a.m. and 9:30 a.m., are blocked off for rounding at UCHealth Yampa Valley Medical Center. "It's important to get out to your team so they know you are accessible," says **Ryan Larson**, director of business development.

Employees are much more likely to contact higher-ups who they see regularly in the department. "It gives us a different perspective on how the employee feels about the work, and the challenges they may have," Larson says.

Recently, ED registrars confided that they were embarrassed at how shabby and outdated the department looked. This led leaders to put in an immediate request for new chairs and carpeting. Leaders are on the lookout for signs that staff are struggling with new processes. Leaders ask open-ended questions ("Do you have any concerns?") to gauge problems. Through closer engagement, patient access leaders learned new information:

- **Employees were not explaining the new process for patient identification properly.** Staff were uncomfortable with the new process, which involved taking pictures of patients. "They felt it was intrusive," Larson explains.

Managers took the opportunity to make an important point: The photos were about patient safety. "Patient identifiers are huge for patient safety. This is one of the fail-safe ways to ensure you have the right patient," Larson says.

Managers offered helpful tips on how to explain the change to patients. Later, an inservice was provided to all employees, since many others also were struggling.

• **Some registrars were struggling to collect because they did not have good information on the patient's out-of-pocket costs.** Another registrar reported difficulty identifying the patient's insurance if there was a secondary plan. Additional training was provided for both scenarios, which focused on how to correctly interpret the patient's benefits.

"We also set goals for point-of-service collection," Larson adds. "We helped staff understand the 'why.'"

For **Jackie Jordan**, MBA, CHAM, visibility in registration areas is the best way to show employees they are valued. "If we consistently add rounding to our leader 'To Do' list, it builds engagement," says Jordan, manager of patient access/central scheduling at Kadlec Regional Medical Center in Richland, WA. This gives leaders an opportunity to identify problems, large and small.

"We take the information we receive and ask ourselves, 'What did we learn?' and 'What issues do we need to resolve?'" Jordan says. During rounding, Jordan says her employees reported a few problems:

• **Internet issues were causing registration delays.** "It ended up being a broken access point. IT fixed it when I told them of the problem," Jordan reports.

• **The greeter was highly stressed due to outpatient services scheduled on the same day each week.** "Administration was able to move certain services to a different day, and provided relief to the greeter for half a day to reduce burnout," Jordan says.

• **Broken equipment.** Employees reported faulty headsets, missing staplers, and jamming printers, all of which were quickly replaced or fixed.

"When we ask the right people the right questions, and follow up, satisfaction will follow," Jordan offers.

The opposite happens if leaders ask several questions during rounding, but never close the loop.

"Employees will likely lose trust," Jordan warns. "They will be less likely to let you know there is an issue in the future." ■

Stop Denied Claims for Patients Discharged With Complex Needs

Some hospitalized patients have complex discharge needs. While many of these needs are clinical, patient access can help with coverage issues.

Communication between patient access and clinical areas "is so very important" when dealing with complex discharge issues, says **Kylie Sokol**, supervisor for hospital admitting services and financial counseling at The Ohio State University Wexner Medical Center.

Clinical and financial counseling teams update each other on possible delays or barriers to discharging patients. For instance, staff sometimes are unable to communicate with the patient because of a medical condition or lack of decision-making capacity. In such cases, says Sokol, "we work closely with the social workers to help in communication with the patient's legal next of kin or family." Sokol personally meets with all newly hired clinical case managers and social workers as part of their onboarding. This ensures that they all understand the financial counselor's role. All available Medicaid programs also are reviewed. Financial counselors are assigned to particular hospital services. "Each clinical team has a dedicated contact for financial questions on behalf of the patient," Sokol notes.

This automatically includes all self-pays who are admitted. "But if an insured patient or a patient's family has brought up questions about their bill or potential out-of-pocket costs, we can see them as well," Sokol adds.

Patient access managers serve on a hospital committee focused on patients with complicated medical needs. Also represented are legal, ethics, hospital administration, and clinicians. Working collaboratively with this group "has created openness and trust," Sokol reports.

The biggest obstacle in discharge planning is lack of insurance. "Sometimes, patients cannot provide information about themselves to us," Sokol says, perhaps because of a medical condition or recent brain injury. "If the family is estranged or unwilling to help, we discuss these patients in committee," Sokol says.

The group determines if the patient needs a court-appointed guardian to help with obtaining Medicaid verifications. These patients often experience complex discharges and need follow-up care. "Patient access can help the team understand potential delays in obtaining coverages for discharge planning," Sokol notes.

In Ohio, patients have to be resource- and income-eligible for Medicaid. Helping patients exhaust resources on allowable items can be challenging.

"Patient access keeps the committee up to date on the progress, or lack of progress," Sokol says. ■

Three Key Areas of Expertise

According to **Karoline Pierson**, director of patient financial care services and patient access at Hennepin County Medical Center in Minneapolis, three skills are most important for the ongoing success of the department:

• Customer service, including de-escalation and strong verbal communication.

"This enables staff to do patient education around the point-of-service financial conversations," Pierson says.

Front-end staff collect more sociodemographic information than in the past. This includes race, ethnicity, and language data. Some patients resist, demanding to know why questions such as "Which category best describes your race?" are necessary.

"Staff need to identify when and how to de-escalate a conversation at the first sign of patient defensiveness or concern," Pierson offers.

Staff explain two things: why the information is gathered and how staff use the data.

"Creating scripting empowers staff to ask the questions diplomatically and confidently," Pierson says. An example of this scripting:

"I am going to ask you some confidential questions. We use this information to provide the best care for every patient" or *"I am going to ask you a few required questions. Some are personal in nature, but all answers are kept confidential. We use this information to provide the best care for every patient."*

Patients usually appreciate knowing the goal is to improve care quality. Many are relieved that the information remains confidential. "This is crucial to ensure accuracy of the data, and alleviate the patients' concerns," Pierson adds.

• Critical thinking.

"I cannot emphasize this enough," Pierson stresses. "Gone are the days of 'dummy' terminals that automatically jumped to the next field."

Today's patient access team works in multiple systems. Staff interpret real-time eligibility results with extensive knowledge of federal regulations.

"They need to problem-solve in the moment, as more and more registration is done at the bedside," Pierson adds, noting that even with standardized workflows, staff still need to think on their own.

• Flexibility.

"This rounds out the staff's ability to weather the constant change that healthcare organizations face on a daily basis," Pierson explains.

Patient access can no longer rely on "the way things have always been done." Technology is continuing to develop. Patients are becoming more discerning consumers.

"We have to be cutting edge, open to change, and able to see things from a different perspective than we did five years ago," Pierson says. ■

COMING IN FUTURE MONTHS

- Train registrars to de-escalate tense encounters
- Use patient feedback to identify registration dissatisfiers
- Discover how happy clinical areas are with patient access
- Implement at-home check-in for surgical patients

HOSPITAL ACCESS MANAGEMENT™

HIPAA REGULATORY ALERT

CUTTING-EDGE INFORMATION ON PRIVACY REGULATIONS

Educate Staff on Criminal Prosecution Risk

Criminal prosecutions for HIPAA violations appear to be increasing, putting both individuals and healthcare organizations at risk for more than just monetary penalties and regulatory burdens.

The criminal penalties for HIPAA violations can be severe: a fine of up to $50,000, imprisonment for up to a year, or both. Additionally, if the offense is committed under false pretenses, there can be a fine of up to $100,000, imprisonment for up to five years, or both.

If the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, the offender can be fined up to $250,000 and imprisoned for up to 10 years, or both.

Those criminal prosecution options are not as well known to healthcare professionals as the civil penalties that are reported often, notes **William P. Dillon**, JD, shareholder with the Gunster law firm in Tallahassee, FL. Office for Civil Rights (OCR) has made 688 referrals to the Department of Justice (DOJ) since the law was enacted. "I think the number of referrals is going to grow as the government focuses more on identity theft," Dillon predicts. "There hasn't been a ton of referrals to DOJ since the process has been in place, but there is reason to think that is going to increase. Covered entities have to have the right processes in place to stay away from that kind of risk."

The criminal sanctions for violating HIPAA were part of the initial public law and are codified at 42 USC 1320d-6, explains **Darci L. Friedman**, JD, CHPC, CSPO, PMC-III, director of content strategy for healthcare compliance and reimbursement within Wolters Kluwer Legal & Regulatory U.S.

There are three prohibitions under the statute. Criminal liability may flow when a person knowingly uses or causes to be used a unique health identifier, or obtains individually identifiable health information relating to an individual, or discloses individually identifiable health information to another person. A person is considered to have obtained or disclosed individually identifiable health information if the information is maintained by a covered entity and the individual obtained or disclosed such information without authorization, Friedman explains.

"Initially, there was some ambiguity as to whether an individual could be criminally liable under the statute and as to whether the term 'knowingly' required proof of knowledge that the conduct was contrary to the statute," Friedman says.

Regarding individual liability, the DOJ concluded that both covered entities and individuals, including directors, officers and employees, may be prosecuted directly under section 1320d-6, Friedman notes.

Concerning the "knowingly" requirement, the DOJ concluded that the element should be read with ordinary meaning to require only proof of knowledge of the facts that constitute the offense and not knowledge that the conduct was contrary to the statute, she says.

"The criminal prosecutions we have seen to date indicate that prosecution is likely where the facts of the case are particularly egregious or where the violation is discovered or prosecuted as part of a larger case involving other kinds of wrongful deeds, like Medicare or tax fraud," Friedman says.

One of the first cases of a HIPAA privacy prosecution involved a cardiothoracic surgeon from China working at a U.S. hospital in 2010, Friedman notes. After receiving a notice of dismissal, the surgeon accessed and read his immediate supervisor's medical records, those of other co-workers, and various celebrities. The surgeon was the first defendant in the nation to receive a prison sentence (four months) for a HIPAA violation.

In 2013, a former nursing assistant at a Florida assisted living facility pleaded guilty to selling HIPAA-protected patient information, including Social Security numbers,

and tax fraud. She was sentenced to 37 months in prison. The crime was discovered when local police executed a narcotics-related search warrant, Friedman notes.

"Most recently, a Massachusetts physician was convicted of a HIPAA violation for her role in a scheme whereby she shared patient information with a pharmaceutical company representative so that the company could target patients with specific conditions," Friedman says. "This case illustrates not only a criminal HIPAA prosecution but the DOJ's ongoing focus on pharmaceutical company marketing practices and their relationships with doctors."

It is important to note that all three cases noted were pursued against insiders, Friedman adds.

"Healthcare providers must ensure, among other things, that employee access to records is limited to the minimum necessary," she says. "Limited access should be paired with following the administrative requirements of the HIPAA security rule regarding the management of the conduct of the workforce in relation to the protection of the information."

Even when criminal prosecution falls on the individual, there still can be significant damage to the healthcare organization, Friedman says. Prosecution of an individual could be a potential flag to enforcement agencies to explore organizational liability.

"Let's not forget that covered entities may be held criminally liable for HIPAA violations as well. When the covered entity is not an individual, principles of corporate criminal liability determine when a covered entity has violated HIPAA," Friedman says. "Even if a case does not implicate the covered entity organization criminally, civil and administrative sanctions, up to and including exclusion from participating in the Medicare program, could come into play. If the organization is a focus, in addition to an individual, it is important that it cooperate in the investigation with regard to the individual in order to be eligible for 'cooperation credit' under the Principles of Federal Prosecution of Business Organizations."

The apparent increase in criminal prosecutions likely is the result of several factors, Friedman says. One factor may be the continuing rise in medical identity theft, and another may be the "Yates Memo," issued by the DOJ in 2015.

In the Yates Memo, then-Deputy Attorney General Sally Yates announced a policy on seeking accountability from the individuals who perpetrated wrongdoing to combat corporate misconduct. The guidance provided in the Yates Memo suggests that U.S. attorneys focus on individuals from the inception of the investigation, Friedman explains.

"Another factor in the increase may be simply that the DOJ is getting used to flexing their HIPAA criminal muscles," Friedman offers. The DOJ memo was issued in 2005, and the first prison sentence came in 2010. Since then, we have seen prosecutions in federal districts in Florida, New York, Texas, Ohio, and Massachusetts."

HIPAA should be a cornerstone of the educational training program for all providers, Friedman says. The training should start when an individual is onboarded and continue throughout the course of their work for the provider organization.

Include in that training information of individual liability, and use recent cases to highlight that liability may include jail time. Criminal prosecution is most likely when an employee in a physician practices knowingly violates HIPAA and the data obtained are used for monetary gain or other illegal acts, **Kyle Haubrich**, JD, an attorney with Sandberg Phoenix in St. Louis.

"It is rare that criminal penalties are handed down by HHS," he says. "Most of the time, the person violating HIPAA does so without knowing that what they did, or didn't do, was a violation. Therefore, you see more civil penalties than criminal ones."

The employer could be held liable in a *respondeat superior* situation, if the employee who was prosecuted was acting on a request to violate HIPAA by his or her employer, Haubrich explains. If the employee acted on his or her own and the employer had no idea the employee was violating HIPAA in a way that caused criminal penalties to be sought, the effect to the employer is reputation-based.

Lack of training and understanding of HIPAA could be contributing to a rise in criminal prosecutions, Haubrich says.

Another cause may be that physicians, healthcare providers, their staff, and even business associates can access multiple records easily with the implementation of electronic medical record software, Haubrich says.

The ability to use the information in a way that could result in criminal penalties (e.g., the temptation to retaliate) is higher.

"Say a physician is fired from a medical practice. However, the practice fails to [revoke] his username and password, allowing him to continue to access the medical records on the EMR software of the practice," Haubrich says. "If that doctor wanted to retaliate against that group for firing him, he could cause all kinds of problems to a

patient's medical record, including changing diagnosis, or worse, using the patient information to open credit cards in the patients' names."

The best way to educate employees about the risk is to educate them on what would cause criminal penalties to be sought, Haubrich offers. If employees know that if they access medical records for no legitimate reason, they could be criminally prosecuted for such access. Employees would be less likely to violate HIPAA because they would know the consequences of doing so, Haubrich argues.

"The best defense is making sure the employees know the risk of violating HIPAA, what criminal and civil penalties could be sought based off of violations committed, and that they, too — not just the physician — can be criminally liable for committing certain violations," Haubrich says. "That can go a long way to helping an employer mitigate the risk of any penalties being handed down."

Dillon suggests emphasizing to employees the significantly increased risk from intentional violations of HIPAA.

"Criminal prosecutions are reserved for intentional acts that cause harm. If you have a nurse who mistakenly faxes a document to the wrong number — that's not a criminal act," Dillon says. "But people who knowingly misuse patient identification need to know that there is this risk, that the government looks on those situations very differently."

The relatively low number of criminal prosecutions may be due to the overall HIPAA caseload facing the government, says **Iliana L. Peters**, JD, shareholder with Polsinelli. Prior to joining the firm, Peters spent more than a decade at OCR, most recently as the acting deputy director and as the senior advisor for HIPAA compliance and enforcement. OCR enforces civil violations of HIPAA, and investigates complaints, breaches, and other HIPAA-related matters that come to its attention.

"OCR expects to receive 24,000 HIPAA complaints in 2018. Further, OCR has received almost 2,400 reports of breaches affecting 500 or more individuals, all of which are posted to OCR's website, as required by the HITECH Act, and investigated," Peters explains.

From there, Peters says OCR refers any complaints or breach reports that may implicate the criminal provisions of HIPAA to the DOJ.

In potential criminal cases, DOJ must prove that an individual knowingly and in violation of HIPAA used, obtained, or disclosed HIPAA-protected information, Peters notes. Although there are penalties for lesser offenses, DOJ likely would take a case in which the agency would have to prove that the individual intended to use the information for personal gain or malicious harm, particularly for identity theft, fraud, or sale of such information. In such cases, DOJ typically adds HIPAA violations to other violations for which DOJ is prosecuting the individual, Peters says.

"Ultimately, healthcare entities themselves can be liable for millions of dollars of civil money penalties after an investigation from OCR. Individuals, including their employees, can be on the hook for criminal penalties of up to 10 years in prison, in addition to a fine," Peters says. "Even if criminal behavior by an employee or an outsider is at issue in a particular case, healthcare entities must be vigilant to protect against such potential criminal behavior by ensuring they implement the administrative, physical, and technical safeguards required by HIPAA, given that they are liable for not doing so."

It is important to remember that criminal prosecution may not start with a standard OCR investigation, says **Patricia Wagner**, JD, an attorney with Epstein Becker Green. In addition to the OCR referral process, it is possible that a HIPAA violation will come to light when the DOJ is investigating or prosecuting another crime and decide to include the HIPAA prosecution as part of the other matter.

When educating employees on the risk of criminal prosecution, Wagner says leaders can describe real incidents in which people have gone to prison for their actions. This makes the risk more than theoretical, she says.

"Often, it is useful to include examples of when penalties have been applied so that employees have a better understanding of the risk," she says. "Of course, it is more important to train employees on and to have a culture of compliance for HIPAA and other laws so that the focus of the organization and employees is on performing tasks in an appropriate manner."

The DOJ memo emphasizes the fact that criminal penalties are reserved for limited and specific violations of HIPAA, notes **Elizabeth Litten**, JD, HIPAA privacy and security officer with Fox Rothschild.

The memo states that such punishment is reserved for violations involving "unique health identifiers' and individually identifiable health identifiers [IIHI]. Thus, the statute

reflects a heightened concern for violations that intrude upon the medical privacy of individuals," the memo reads.

The DOJ memo focuses on violations by covered entities and notes that when a covered entity is a corporate entity, the conduct of agents may be imputed to the entity when the agents act within the scope of employment.

Criminal liability of a corporate entity may be attributed to individuals in managerial roles, Litten explains.

Once a HIPAA violation is referred for criminal prosecution, the case may be easy for prosecutors.

"It may be that a DOJ conviction for a knowing violation of HIPAA is more easily obtained than a conviction for a violation of other federal laws governing healthcare providers, such as Anti-Kickback Statute violations," Litten says. "In addition, where a healthcare entity, like a large hospital system or health plan, has deep pockets, the OCR may pursue very high civil monetary penalties and rely on the financial implications as a deterrence message sent to the regulated community. DOJ may seek to deter behavior associated with a wider range of criminal activities by pursuing jail time for a HIPAA violation. I expect HIPAA will be used as the basis for criminal prosecution where other, less easy-to-prove criminal conduct is involved, similar to convicting mafia members for tax evasion." Although criminal prosecution may seem extreme to those accused of HIPAA violations, it may be far more mundane to prosecutors, Litten says.

"Be aware that a HIPAA violation involving disclosure or breach of IIHI may be the low-hanging fruit for criminal prosecutors originally focused on other violations of law," Litten warns. "In particular, covered entities should carefully evaluate arrangements with third parties that involve the sharing of IIHI with third parties for commercial/personal gain or commercial harm, since the highest criminal penalties under HIPAA are for violations committed with the intent to use or disclose IIHI for these purposes." ■

Federal Court Affirms No Private Right of Action

A federal judge recently affirmed that HIPAA does not provide a mechanism for individuals to sue when they believe their privacy rights have been violated. However, the decision probably will not stop individuals from thinking they have the right to sue.

The supposed private right to action under HIPAA has confused people since the law's inception, explains **Nathan A. Kottkamp**, JD, a partner with McGuireWoods.

The case involved a plaintiff who had been treated at a Washington, DC, hospital in 2017, during which staff instructed her to complete an online form at a computer workstation. The plaintiff thought the information could be seen by other patients in the area. She filed complaints with HHS, the hospital, the laboratory testing company the hospital used, and the District of Columbia Office of Human Rights. She claimed that the hospital and lab company failed to make proper public accommodations for patients.

The federal court recently followed the pattern of previous courts by telling the plaintiff HIPAA does not allow such lawsuits from individuals. The courts have been clear in confirming there is no private right of action, which means a healthcare entity cannot be sued for a HIPAA violation by a patient, Kottkamp explains.

"That is often a huge surprise to members of the public. They see HIPAA information all the time, and they often are shocked to think that if this is such a big, important federal law, why can't I sue if I believe my rights have been violated?" Kottkamp says. "I probably get an average of a call a month from people who believe their HIPAA rights have been violated, and they want to sue. I have to tell them, 'Sorry, there's nothing you do can other than filing a complaint with the OCR.'"

Plaintiffs also have tried to use HIPAA violations as a starting point for other lawsuits related to privacy matters, essentially saying HIPAA represents the most fundamental level of privacy patients should expect. If there were HIPAA violations, plaintiffs often believe there were de facto violations of more strict state privacy regulations. Those cases have not been very successful, either, Kottkamp says.

"Providers need to know that a patient's inability to sue over HIPAA violations is no reason to be lax about compliance. Sometimes, the reputation damage and exposure in the media can be more costly than any civil penalties you might have incurred," Kottkamp warns. "If someone goes on social media and says you don't care about patient privacy, that could be very costly." ■