HOSPITAL ACCESS MANAGEMENT™

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

INSIDE

RELIAS MEDIA

MARCH 2020 Vol. 39, No. 3; p. 17-24

Many People Put Off Medical Care Because They Cannot Pay High Deductibles

Patients often find out about a high deductible not from their insurer or employer, but from a registrar — and many of these high-dollar accounts go unpaid. Now, multiple recent studies show that people are avoiding care because they cannot pay their high deductibles.

"It is not unusual to hear from patients that they are struggling to afford medications or not taking them as prescribed. As deductibles continue to rise, we're only going to hear this more," says **Adam Gaffney**, MD, MPH, an instructor in medicine at Harvard Medical School.

People with COPD and high-deductible plans were more likely to delay care compared to those with traditional health plans, according to the authors of a recent study.[1] Researchers compared 803 people with high-deductible plans to 1,334 people with traditional plans. They fully expected high deductibles to cause nonadherence with medications and greater financial strain. They did find both of these things.

"However, one surprising finding was just how many patients are affected," says Gaffney, lead author of the study. Most people with high deductibles faced financial hardships despite being employed. They also recorded more ED visits and hospitalizations, something that seems counterintuitive.

Typically, deductibles keep people away from the hospital. "But this may not be the case for chronically ill patients who deteriorate when they don't take needed controller medications," Gaffney observes.

When people avoid medical care because they cannot afford the deductibles, they may end up in the hospital because of it. "The current system is simply not working for those with expensive, chronic illnesses like COPD," Gaffney concludes.

Cancer survivors with high-deductible plans were more likely to delay or avoid care compared to those with traditional plans, according to recent research.[2] The authors of a third study found that people with consumer-driven health plans (a type of high-deductible plan) use fewer services than those enrolled in traditional plans.[3]

"Perhaps most interestingly, this was even the case among those with chronic conditions," says **Bill Johnson**, PhD, the study's lead author and a senior researcher at the Health Care Cost Institute.

Here, three patient access leaders report on how they are addressing the problems caused by high deductibles:

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: Jason Schneider
EDITORIAL GROUP MANAGER: Leslie Coplin

• **Kaylin Fogarty**, director of patient access and financial coordination at Tufts Medical Center, a 415-bed Boston-based academic medical center: The majority of commercial plans we see have a deductible as part of their cost-sharing. Some plans have tiered benefits, with different deductible, copay, and co-insurance amounts, depending on the provider or facility. It can be difficult for patients to understand which tier their provider falls in — and therefore, what their cost-sharing will be.

The best thing we can do to help patients is to communicate their expected out-of-pocket costs. Many patients do not understand their benefits fully. The more we can do to educate them on their plan, the more empowered they will be.

If a patient has a deductible, we offer no-interest payment plans to help manage these costs. Our customer service team will work with the patient to agree upon a monthly amount based on the total outstanding balance.

We reach out to patients to inform them of their expected out-of-pocket costs for certain services, such as surgeries and radiology exams. We hope to expand that proactive outreach to more patients who are receiving less expensive services, but would still benefit from understanding costs preservice.

Financial conversations can be sensitive. We strive to communicate this message so as to educate patients about the impending costs, but not deter them from receiving the care they need.

When patients are able to plan ahead, the hospital is more successful in obtaining payment. Patients are grateful to know the costs prior to receiving the services. Nobody wants to receive an unexpected, surprise bill weeks after receiving healthcare services.

• **Pamela Carlisle**, MHA, FHAM, director of revenue cycle management at Zanesville, OH-based Genesis HealthCare System: We are seeing an increase in retiree benefit plans with high deductibles, as well as small employer plans. High deductibles are often hidden from the patients. They do not understand the changes that have occurred with their specific plan.

We have found that it is critical to have conversations with the patient prior to their service date. We not only work with the patient, we conference in the employer so everyone can remain on the same page and we all understand the cost moving forward. This allows the patient to ask pointed questions to the employer, keeping the provider out of the discussion.

We have found that truly reviewing the details with the patient has been essential. It is not just giving them a number. We explain how we got to that number, and how we can help them satisfy their portion. We have, in turn, seen an increase in employee payroll deductions and payment plan options.

Timing is everything. Obviously, it is best to do all the prework, but there are many situations where that cannot occur — ED visits, walk-ins, and add-on procedures.

We pride ourselves in timely follow-up for financial screening. Early on, we identify patients who need follow-up calls. We then make every effort to ensure we provide them with the tools needed to take care of their financial commitment. It could be a phone call post-appointment or speaking to an approved family member on the day of service.

We start by saying, "We want to review the details of your insurance plan with you. Your insurance has confirmed that, through your employer, these are the benefits assigned."

As providers, we are processors of information. We do not determine the factors involved in benefits. But that is a hard concept for our patients to

understand. It is our role to assist them with understanding their plan benefits, the cost of the procedure and their out of pocket, and to be able to identify any finance assistance that can be provided. As the revenue cycle, we take care of the financial health of the patient.

• **Julie Johnson**, CHAM, FHAM, director of health information management and patient access at Mount Graham Regional Medical Center, a 49-bed acute care hospital in Safford, AZ: We are seeing an increase of outstanding balances that go to bad debt. Most patients are unable to pay the high deductibles. They will always owe the full amount when obtaining exams such as ultrasound or MRI.

The cost of the test is often less than the deductible. A patient may come in toward the end of the year, and owes $3,000 on their deductible. The price of an MRI could be $2,100. All of that would go to the deductible, and they would be responsible for payment.

This is why we offer the choice of a self-pay radiology discount. We do inform patients that with this option, it does not go toward their deductible. Instead of paying $2,100 for the MRI, the patient elects to pay the cash price, which is much less. The service is not submitted to insurance, saving them money.

Most patients want to be informed about the price prior to receiving services. Staff preregister scheduled patients, give estimates, and inform the patients of the different options available to them. All staff are knowledgeable on discount policies and our charity care program, and promote them to patients.

Some ask for discounts or cash pricing. They state, "We can't afford this," and ask if we will accept 50%. These requests go to the vice president and CFO for approval. We do have five insurances that do not allow discounts for their insured.

Our financial counselor is now located right in the patient access department. Previously, her office was in a building behind the hospital.

To make payment arrangements or apply for charity or other programs, the patient would have to walk out of the hospital to their car and drive around to the back of the hospital.

We moved the financial counselor to the front end. She is now steps away from any registration area. At the same time, we moved our inpatient authorization employee to the patient accounting office, where they work closely with the billing personnel. This musical chairs approach has worked well for us.

We assure the patient that we are willing to work with them. We show compassion and empathy, yet we are consistent and enforce the policies we have in place. ■

REFERENCES

1. Gaffney A, White A, Hawks L, et al. High-deductible health plans and healthcare access, use, and financial strain in those with COPD. *Ann Am Thorac Soc* 2020;17:49-56.
2. Zheng Z, Jemal A, Banegas MP, et al. High-deductible health plans and cancer survivorship: What is the association with access to care and hospital emergency department use? *J Oncol Pract* 2019;15:e957-e968.
3. Johnson W, Milewski A. Lower health care spending and use for people with chronic conditions in consumer-directed health plans. Health Care Cost Institute Brief; May 2019. Available at: https://bit.ly/2RUj4kp. Accessed Jan. 27, 2020.

Expensive Deductibles Bringing Many Changes to Revenue Cycle

If it seems like many more patients are presenting with high-deductible insurance plans, there are some hard data to back it up.

Almost half (47%) of commercially insured patients younger than age 65 years now carry a high-deductible plan (defined as at least $1,350 for individual coverage, or $2,700 for family coverage), according to the authors of a recent study.[1]

"What we're seeing with high-deductible health plans aligns pretty well with this. This is a huge population to accommodate," says **Austin Brandt**, director of revenue cycle solutions at Bluetree Network, a health IT consulting firm. Even so, the total dollars paid by patients remains a relatively small portion of total A/R for most hospitals. "It hasn't completely jolted us out of the 'treat now and bill later' mentality," Brandt observes.

High deductibles are negatively affecting hospitals' financials, Brandt reports. Many patients cannot pay them, so the accounts end up written off or become bad debt.

"The truth is, there's so much room for improvement that almost anything that encourages collections earlier in the revenue cycle is a step in the right direction," Brandt explains. Patients with high deductibles often need an expert's help. Ideally, this means a highly trained financial counselor who handles such cases all day.

"No matter the size of the organization, there are always more

patients than financial counseling staff can proactively reach out to," Brandt laments.

That is where front-end staff come in. Registrars can pave the way for the eventual discussion with a financial counselor.

"Every time you schedule or register a patient is an opportunity to discuss payment expectations and available assistance," Brandt offers. When the patient does meet with the financial counselor, the basics are covered already. The discussion can focus on available options, such as zero-interest bank loans.

"By guaranteeing the loans and eliminating credit checks, you open up funding to a huge population of patients," Brandt notes. This is beyond the scope of the average registrar, but any registrar can at least start the conversation. Putting the right tools in the hands of financial counselors also is important.

"They need to prioritize patients through different measurements, like propensity to pay, to maximize their effectiveness," Brandt adds. ■

REFERENCE

1. Martinez ME, et al. Health insurance coverage: Early release of estimates from the national health interview survey, 2018. National Center for Health Statistics. Available at: http://bit.ly/38D4rse.

Multiple Bills Cause Confusion, Many Complaints

At Orlando (FL) Health, revenue cycle leaders were hearing many similar complaints from patients who received multiple bills after their hospital stay. Many had received other bills and paid them in full.

"Patients who had multiple services within a narrow timeframe were confused," says **Michele Napier**, vice president of revenue management and chief revenue officer. Sometimes, bills included the same dates of services, but were from different providers. Napier's department decided to make a big change by creating a "uni-bill."

"All hospitals and physician charges are combined into one statement for the patient," Napier reports.

More patients are paying outstanding balances on time. Napier attributes this to less confusion on whether the amounts are correct. "Patients who understand their bills are more likely to pay," she observes.

At Indiana University (IU) Health, many patients were "overwhelmed and confused" because they received multiple billing statements, says **David Burton**, vice president of revenue management.

Some patients complained about bills for physician services when they had already paid for an associated inpatient stay. Others received multiple bills for one ED visit and assumed they were being double- or triple-billed.

However, that was nine years ago. At that time, the health system switched to a consolidated patient statement.

"The statement clearly shows patients the amount charged for all physician and facility services," Burton explains.

This change was developed in-house since few, if any, vendors offered this kind of solution.

"Integrating two completely different patient accounting systems was a tremendous technical challenge," Burton recalls.

The systems did not share a single unique patient identifier. Revenue cycle leaders had to build an algorithm that could match the same patient and guarantor combinations across platforms.

"We also had to develop a payment allocation methodology," Burton adds.

A single payment would need to be dispersed to multiple providers with separate bank accounts. "We also wanted to link related hospital and physician invoices so patients could see all of the bills related to their inpatient stay or outpatient procedure," Burton notes.

That link did not exist, so an algorithm was needed to develop it. "The database and programming that support our consolidated patient statement are complicated components of our revenue cycle IT infrastructure," Burton says.

The consolidated patient statement includes a single minimum monthly payment, an "at a glance" summary of all account activity (insurance payments, adjustments, and patient payments), and a "What You Need To Do" section explaining the next steps. Almost immediately, there was much less confusion over hospital bills. IU Health received payments faster, with fewer calls to customer service.

"It was clear the unified statement helped patients better understand what they owed and for what services," Burton says.

IU Health also put an interactive voice response system in place. "The system allows people to make electronic payments in a way that is most convenient for them and on their schedule," Burton explains.

For patients, it is one more way to access their account or make payments by phone or online.

The health system held patient forums across the state to obtain feedback on all the changes.

"Across the board, patients were pleased to be able to see their services and charges together," Burton says. "It

provided more clarity into how they were being billed."

People also appreciated receiving less mail and fewer separate payments to track. "We continue to gather feedback about billing procedures," Burton adds.

Revenue cycle leaders ask the hospital's patient and family advisory committee for input, too. "The most recent feedback pointed to the need for self-service payment online," Burton reports. The health system is looking to expand these options. Patients can make payments online by enrolling in IU Health's patient portal, but want the ability to pay through email or texts.

"Patients continue to express a desire for convenience," Burton says. ■

Study Groups and Quizlets: Earning CHAA Is a Team Sport

Few registrars at Connecticut Children's Medical Center in Hartford had earned the Certified Healthcare Access Associate (CHAA) credential, offered by the National Association of Healthcare Access Management (NAHAM). Now, it is required for advancement.

"Our team members' interest in the CHAA has grown tremendously," reports **Jessica Budri**, RN, MSN, APRN, senior manager of patient access.

The patient access career ladder includes three levels: Level 1, Level 2, and Team Lead. Employees hired as Level 2s must earn a CHAA certification within a year. They also are required to complete the following:

- Participate on at least one hospital committee outside their immediate department;
- Cover other patient access areas as needed;
- Train new team members.

Registrars pay for the exam, which is difficult for some. However, the department reimburses the cost once registrars pass.

"That has certainly motivated and increased our testing rates," Budri reports.

Registrars who are new holders of the CHAA certification have a lot to look forward to. These employees:

- are publicly congratulated in the department newsletter;
- receive a personal card signed by department leaders;
- can add the CHAA credential after their names in their email signatures;
- are listed in the newsletter of the New England chapter of NAHAM. "That is very cool because it goes out to all NAHAM members in our region," Budri notes.

Before the department made these changes, registrars expressed little interest in earning a CHAA certification. The main problem was lack of enthusiasm. "Employees did not really see the importance of a certification for their career," Budri explains.

Only financial counselors and the authorization team took the exam because it was a job requirement for those roles. "There was no incentive for anyone in patient access to get the CHAA," Budri recalls.

Anyone who did take the CHAA had to go it alone. Managers asked their Level 2 employees to make it a group effort instead. As part of their career ladder requirements, the Level 2s formed CHAA study groups. Right away, attitudes changed. "Employees know they will be supported up until the exam," Budri says.

Many patient access staff earned the CHAA and advanced to Level 2 status. This caught the attention of Level 1 employees.

"They see it's a way to be taken more seriously in the department," Budri observes. "They have taken it upon themselves to get the certification." Budri led by example, and obtained a Certified Healthcare Access Manager (CHAM) credential, adding to the momentum.

Before the department made the CHAA a requirement in March 2019, only 16 employees had earned the credential. "Since then, an additional 11 have gotten the CHAA," Budri reports.

The surge in CHAA credentials has jump-started other changes. Newly certified registrars are highly motivated to choose patient access as a career. Many are networking with peers in the field online for the first time. "It has greatly increased engagement," Budri says. "Employees now see the potential for growth in their position."

Lucianna Easton, CHAA, went even further by becoming involved on the national level (she joined NAHAM's membership committee). As one of the Level 2s charged with forming study groups, Easton's first step was to create flashcards. "This helped get the momentum going," Easton says.

Next, all participants took a practice test to identify their trouble spots. Vocabulary definitions were a big focus, not because they are included on the CHAA exam (they are not) but because they are necessary to understand the questions asked.

Outside of study groups, employees prepared for the test in their spare time. "While we try our best to study at work, there is a certain amount of initiative that needs to be taken outside of work," Easton notes. Many registrars relied heavily on scenario-based questions on

Quizlet.com, which are similar to those on the CHAA exam.

Easton urges colleagues to take their time when sitting for the exam. During her own CHAA exam, passed on the first attempt, that is exactly what she did. "I utilized the whole two-hour testing timeframe. I was the last individual in the room," she says.

Registrars must see the big picture. "A patient access department has to have a mission and vision on why CHAA is important," says **Cheryl Barrett**, director of patient access at Parkland Health & Hospital System in Dallas. Even so, registrars want to know what is in it for them. Some already want to advance in the field.

"But for short-term employees who don't plan to build a career in patient access, becoming certified may not be as important," Barrett acknowledges. Currently, fewer than 10% of registrars have earned their CHAA. The department recently started group study sessions to increase this percentage dramatically.

For managers, securing buy-in from a smaller group of motivated employees is easier than trying to convince an entire department. For registrars, camaraderie is an important motivator. "Patient access employees befriend one another," Barrett notes.

Sessions are held at convenient times, at the start or end of a shift, and limited to 30 minutes.

"By keeping the sessions short, employees see that it does not have to impinge too much on their personal time," Barrett explains.

The single best approach they have found for training sessions: To cover material that is relevant to both the CHAA exam and the employee's job.

"Then, the time spent becomes a win for both the employee and the organization," Barrett says. ■

Is Registrar Friendly? This Can Be More Important Than Other Tangible Metrics

Niceness cannot be measured in the same way as the number of calls taken per hour or the percentage of copays collected, but it still needs recognition. Oklahoma City-based INTEGRIS Health made some changes to reward their friendliest registrars:

• Employees are rated on how they come across to patients and families.

"The employee is then provided real-time feedback, including tips to improve," says **Veronica Hughes**, administrative director for patient access.

• Calls with patients are recorded and evaluated.

This has been ongoing for years at the centralized call center, but will soon be expanded. "We will be transitioning toward a more robust phone recording evaluation system," Hughes says. The new system will give real-time reports on the tone of voice used by registrars.

• Each day, leaders send a "kudos" email on registrars who gave exceptional customer service.

"This is stored in the employee's file, and referred to during annual performance reviews," Hughes says.

• Anyone who consistently gives exemplary service is considered for a promotion.

"All employee recognitions are shared at monthly meetings," Hughes adds.

Most patient access leaders really do not need metrics to tell them who their most helpful registrars are. The trick is how to retain these high-value employees.

"We must connect with them on an individual level," says **Susan Milligan**, patient experience director at Ensemble Health Partners in Mason, OH.

There are no shortcuts. Patient access leaders put in plenty of face time. "Learning what's important to them is critical," Milligan stresses.

"One of the best things you can do is ask questions." Ensemble uses employee recognition questionnaires to identify:

• how the employee wants to be recognized (privately or publicly);

• whether they prefer email or verbal recognition;

• what they want, specifically.

"Maybe it's their name in lights on digital signage in the lobby, for all to see," Milligan says. Others really want a handwritten note, a gift card, their favorite candy bar, or the opportunity to coach their peers.

"We empower our associates to think outside the box. When it pays off, we encourage them to share what's worked," Milligan shares.

Managers spend lots of time in the department talking with employees. They pick up on who really wants to advance in the field.

"If they aspire to lead teams or improve processes, we explain that coaching is a core function," Milligan says.

New hires work alongside the customer service stars.

"We use top performers for side-by-sides so they can learn from the best," Milligan says.

A simple thank you goes a long way for almost all registrars, and the details count.

"We want the associate to know exactly what created the positive experience so the behavior continues," Milligan explains. ■

A Little Coding Knowledge Goes a Long Way Toward Preventing Denials

In years past, patient access had little or no knowledge of coding. This has changed.

"As payment models and coding requirements change, more training is necessary," says **Jannifer Owens**, revenue cycle content manager at St. Paul, MN-based 3M. True coding expertise comes from structured training in anatomy and physiology, successful completion of a coding exam, and years of experience, Owens says. Patient access staff need far more limited knowledge of coding to perform their jobs. However, it is vital that they learn some basic skills. "Patient access is the first line of defense from a payment perspective," Owens notes.

Above all, patient access needs a good understanding of medical necessity and why claims might be denied. "Staff should also have knowledge in other areas, such what's required on an order and what requires an authorization for payment," Owens says. They also need to understand Advance Beneficiary Notices and modifier requirements. "They wouldn't need to be an expert," Owens says. "But they do need to have the skills to ensure compliance."

From a medical necessity perspective, if incorrect diagnosis codes are used, a claim is going to be denied. "This means that it generally will come back to billing, then coding, then potentially the provider," Owens explains. At the very least, this delays payment for weeks or months. It is always possible the reworked claim ultimately will be paid. "But the cost of working the denial may outweigh the payment from the initial test, study, or procedure," Owens cautions.

Different payers use different requirements for medical necessity.

"Staff need to have access to medical necessity software for a variety of payers, or at least know how to search for the information," Owens suggests. Sometimes, a specific test is ordered and conducted, but no valid diagnosis is present to support the test. This often happens with Medicare denials.

"Medicare has coverage determinations that instruct staff on what codes will pay for which procedures," Owens explains.

To train patient access staff in coding skills, clearly identified expectations are essential. "You are not looking to make the patient access staff coders," Owens explains. "You are training them to recognize, understand, and act on areas of impact." ■

Peer-to-Peers Not Always Successful; Patient Access Can Increase the Odds

Payers are increasingly asking for peer-to-peer conversations. This requires the patient's physician to take time out of his or her busy schedule to discuss the case with the payer physician.

"Peer-to-peers are happening much more than in the past," says **Ronald Hirsch**, MD, FACP, a physician with Chicago-based R1 RCM Physician Advisory Solutions. The main reason behind the surge in peer-to-peers is that health plans are seeking to avoid paying a hospital bill for an inpatient admission.

"If a peer-to-peer is needed, the next question is who should do it," Hirsch explains.

If it is a question of the medical necessity for the procedure, the physician is best-suited to participate. "They are aware of the indications and other therapies that have been tried," Hirsch observes.

Sometimes, the question is more about the patient's status as an inpatient or outpatient.

"Most practicing physicians have little understanding of the nuances of this," Hirsch says.

Hospitals work with multiple payers, and each uses a different method to determine the patient's status.

"Expecting the physician to understand that is unreasonable. And that is where the hospital's physician advisor should be utilized," Hirsch offers.

Patient access is not conducting the peer-to-peer, but can facilitate these requests. To do so, says Hirsch, "patient access should have a close working relationship with the physician advisor."

There is no guarantee the payer will overturn the denial, even after the peer-to-peer happens. Success rates for these calls varies widely.

"Several variables affect the outcome," Hirsch notes.

It all depends on how willing the payer's physician is to listen.

"Many insurance medical directors already have their mind made up before they take the call," Hirsch says. "Nothing will convince them to change it."

Other payer physicians are willing to hear the hospital's viewpoint. Some conclude the initial decision to deny the claim was made with limited information.

"Once the physician, or physician advisor, fills in the gaps, the claim gets approved for payment," Hirsch says.

In 2015, Ensemble Health Partners revamped its processes in response to a surge of payer requests for peer-to-peers. Physician advisory, virtual utilization review, and bedded insurance authorization teams were created. These groups are responsible for:

- reviewing level of care/patient status for appropriateness;
- identifying if medical necessity guidelines are met;
- following up on medical necessity denials and peer-to-peer requests.

Payers are not making it easy. Already-short timeframes from payers to complete the peer-to-peers are shrinking, says **Kathy White**, AVP of virtual utilization review and bedded insurance authorization.

Busy attending physicians have no time for the lengthy phone calls.

"Some payer contracts require the attending to perform the peer-to-peer," White notes. These specify that the physician advisor is not allowed to do so.

For patient access, there are two main challenges: tracking that the peer-to-peer was completed, and tracking the outcome (whether the denial was upheld or overturned). This is a time-consuming process that diverts patient access staff from other tasks.

"There is an administrative strain on staffing to complete the full process of scheduling, documenting, and determination," White says.

Ideally, fewer peer-to-peers are requested. Patient access does its part by obtaining authorizations for scheduled cases. Thorough documentation in the medical record gives the payer no reason to ask for the peer-to-peer in the first place. "We track this at the physician level, looking at progress notes and quality documentation," White says. ■

COMING IN FUTURE MONTHS

- Switching from manual to automated auths is not easy
- Revamping QA with data from recorded phone calls
- Registrars struggling with Medicare beneficiary IDs
- New evidence shows prior authorizations harm patients

HOSPITAL ACCESS MANAGEMENT™

HIPAA REGULATORY ALERT

CUTTING-EDGE INFORMATION ON PRIVACY REGULATIONS

Expect More High-Tech Breaches, Attorney General Audits This Year

The trend for HIPAA compliance is toward more breaches and complex breaches than seen in earlier years of efforts to follow the privacy rule, say some experts. A sharp increase in cyberattacks also may be coming this year. Most HIPAA breaches in the past were of a rather low-tech nature, even if they involved lost computers and data files. Laptops were stolen, jump drives were lost, and paper documents were mishandled. But that is changing now, partly because the digital revolution has completely changed how healthcare organizations handle data, says **Steven Marco**, CISA, ITIL, HPSA, president and founder of HIPAA One, a consulting group in Lindon, UT.

"It used to be that the breaches were not very frequent. When they happened, they often involved the theft of electronic media. That type of physical data loss represented your highest likelihood of having to report a breach," Marco says. "Server incidents were almost unheard of. We've seen a drastic change with a trend toward each incident involving more individuals, rather than many incidents involving a small number. Each cyber incident now typically involves tens of thousands of individuals. That trend is not changing any time soon."

The nature of attacks on covered entities is changing at the same time, says **Bobby Seegmiller**, senior vice president and founding partner of HIPAA One. Healthcare organizations have become much savvier about how to protect their data from outside threats, but they still struggle with internal security, he says.

"Some of these hospitals are like Fort Knox with all the security they have to keep someone from coming in either physically or through a cyberattack — but their own employees are leaving the back door wide open," Seegmiller says. "The hospital puts up all this security and it is undermined by the employee who opens an email and responds to a phishing attack."

Employee training is critical, but that is not enough, Seegmiller stresses. It is important to test employees periodically with a real-world scenario such as sending a fake email that includes all the hallmarks of a phishing attempt and see who takes the bait, he says. "We're finding that about one in three will click on the link," he says.

Marco predicts that cyber security attacks will increase by 50% in 2020. "There is an industry for cyber criminals that did not exist years ago. There is a market on the dark web for financial information and private information that is driving these criminals to work harder and find new ways to access this product they need to sell," Marco observes. "We will see more use of ransomware also, because organizations are paying the ransom, and the criminals know that every hospital needs to make payroll. If [criminals] see that it works, they will keep trying to get ransomware into your systems."

Marco also notes there have been ransomware attacks in which the healthcare organization refused to pay the ransom and did not report a breach, but still accessed data from backups. In those cases, the danger may not be over if the hackers could access protected data.

"I would anticipate that these hackers will get frustrated and eventually start releasing PHI [protected health information] from those organizations that did not pay," Marco says. "Any organization in that position should be prepared for that possibility and have a plan in place for responding. It is possible that any patient whose PHI was released could complain to Health and Human Services, and it's now a reportable breach."

New compliance requirements also are possible in 2020. This will put added stress on covered entities to bolster their HIPAA protections at the same time they need to do more to protect themselves against cyberattacks, Marco explains.

"There's a big push for privacy right now, and there is a good chance HIPAA will be amended to align with the public sentiment in favor of patients having more control over their health information," he predicts.

Seegmiller notes the likelihood of undergoing an Office for Civil Rights audit also has increased in recent years. The rate of

audits several years ago was so low that covered entities believed they would never be audited and grew lax in some areas of compliance, particularly the risk assessment requirement, he explains.

"We're seeing a new trend with state attorneys general, who were deputized in the HITECH Act in 2009 to conduct these audits, getting more interested in HIPAA audits. It may be because they saw that the feds were collecting all these penalties from their audits, even though they were infrequent, and they saw a chance to get in on that," Seegmiller observes. "It's a revenue source. We're seeing more attorney general audits that we didn't see in the past."

Marco notes there are simple steps for improving HIPAA security that often are overlooked. For example, the commonly used Microsoft Office 365 software includes privacy and security options that can be effective in reducing vulnerability to cyberattacks, but covered entities do not activate them, he says. Using two-factor authentication also can be highly effective in deterring fraudulent logins, Marco adds. This method usually requires sending a simple code to the authorized user's mobile phone to verify the person's identity before completing the login process.

"Multifactor authentication with a code sent by text message wards off 99.999% of attacks trying to compromise user accounts," Marco says. "That's a huge measure of safety that requires little investment or effort." ■

HIPAA Settlements Hold Lessons on Right of Access, Breach Reporting

The Office for Civil Rights (OCR) recently announced two HIPAA settlements that offer lessons for covered entities regarding right of access and failure to notify after a breach.

In early 2019, OCR announced it would take steps to enforce the rights of patients to receive copies of their medical records timely and at a reasonable cost. This led to the introduction of the HIPAA Right of Access Initiative.

In September 2019, OCR issued a penalty to Bayfront Health St. Petersburg, FL, a fine of $85,000.[1] This was the first enforcement action and settlement under this new initiative. In December, OCR settled a second case, this time with Korunda Medical in Florida, which agreed to take corrective actions and pay an $85,000 fine.[2]

In a press announcement about the Korunda settlement, OCR explained the Right of Access Initiative was the agency's promise to "vigorously enforce the rights of patients to get access to their medical records promptly, without being overcharged, and in the readily producible format of their choice."[2]

The settlement addressed a patient complaint alleging Korunda failed to forward a patient's medical records in electronic format to a third party despite numerous requests. "Not only did Korunda fail to timely provide the records to the third party, but Korunda also failed to provide them in the requested electronic format, and charged more than the reasonably cost-based fees allowed under HIPAA," OCR said.[2] "OCR provided Korunda with technical assistance on how to correct these matters and closed the complaint. Despite OCR's assistance, Korunda continued to fail to provide the requested records, resulting in another complaint to OCR."

Ryan Meehan, healthcare senior manager of Schellman & Company, a global independent security and privacy compliance assessor based in Tampa, FL, explains that the regulation from which these cases and fines are emerging can be traced to the HIPAA Privacy Rule requirements under §164.524, which concerns an individual's access to protected health information.

Specifically, he says, these cases seem to revolve around the requirement that "the covered entity must permit an individual to request access to inspect or to obtain a copy of the protected health information about the individual that is maintained in a designated record set. The covered entity may require individuals to make requests for access in writing, provided that it informs individuals of such a requirement."[3]

"While the Bayfront case focused on significant delays — nine months when the standard requires it to be submitted in the proper format within 30 days — the Korunda case is notable in that the format in which the files were eventually provided to the individual was not appropriate and the cost to the individual for access to their ePHI was not reasonable," Meehan says. "The OCR came in to provide technical assistance after the initial complaint was received, but the case had to be reopened as Korunda was still noncompliant. This is the first case in which the format and cost are being considered and factored into a fine from the OCR."

In looking at the fines Korunda received, Meehan says it is worthwhile for risk managers and compliance officers to revisit the HIPAA requirements on which the fine is based. He cites these provisions:

- Privacy Rule § 164.524(b)(2)(i): "…the covered entity must act on a request for access no later than 30 days after receipt of the request as follows";
- Privacy Rule § 164.524(c)(2)(i): "The covered entity must provide the

individual with access to the protected health information in the form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable hard copy form or such other form and format as agreed to by the covered entity and the individual."

• Privacy Rule § 164.524(c)(2): "If the individual requests a copy of the protected health information or agrees to a summary or explanation of such information, the covered entity may impose a reasonable, cost-based fee."[3]

While there are defined exceptions noted within the standard, Meehan says "it is clear that the OCR is taking seriously the effort for individuals to access their ePHI. In the case of Korunda, this is now extending beyond just the timeliness of those individuals receiving their ePHI; it also extends to include the format and cost associated with the request."

Meehan stresses the importance of reviewing how individuals might request information and if the organizations can meet those requests appropriately. "Decide whether there is confidence that the records can be provided timely, that the records are kept in an appropriate manner that has been defined and known by the individual, and that there is a justifiable and reasonable cost associated with providing those requests to the individual," Meehan explains.

The key takeaway from the Korunda settlement is the necessity of respecting basic compliance obligations, says **Matthew R. Fisher**, JD, partner with Mirick O'Connell in Worcester, MA. When considering the individual right to access, the right has been around as long as the privacy rule, he notes. Further, the parameters around access are clear, he says. Thus, delaying a response or giving an individual a runaround is not something that should occur.

"OCR had been making a number of public comments about focusing on the right of access. Finally getting two settlements in that regard should not have been overly surprising," Fisher offers. "The message being sent is that if organizations continue not honoring the right of access, then enforcement will follow."

Fisher notes the relatively small dollar amount of the fines, wondering "whether a sufficient message of deterrence has been made."

OCR also may be sending a message with the settlement amounts in both right to access cases, says **Matt Frederiksen-England**, CHC, CHPR, CHRC, faculty member at Walden University in Minneapolis. He notes Bayfront is a level II trauma tertiary care, with about 480 beds and more than 550 physicians, while Korunda is a much smaller provider, seeing about 2,000 patients per year. "OCR has now applied the same fines to both a large institution and a smaller provider-based office," he says. "OCR is making a statement showing they will hold all accountable to the HIPAA Privacy Rule requirements regardless of size."

The Korunda settlement signals OCR is taking a much stronger approach to making sure patients can access their information, says **William P. Dillon**, JD, shareholder with Gunster in Tallahassee, FL.

"OCR wants it to be clear that patients have a right to get access to their records, and in an appropriate format," Dillon says. "You don't have to go out and buy special software, but if it is feasible to give patients the data in the format they want, you have to do it because OCR is not going to tolerate a failure to give patients access to their data." ■

REFERENCES

1. HHS.gov. OCR settles first case in HIPAA Right of Access Initiative, Sept. 9, 2019. Available at: http://bit.ly/2GuUEsj.
2. HHS.gov. OCR settles second case in HIPAA Right of Access Initiative, Dec. 12, 2019. Available at: http://bit.ly/2uImjmJ.
3. HHS.gov. Individuals' right under HIPAA to access their health information 45 CFR § 164.524. Available at: http://bit.ly/2RzGD2X.

Wrong Person Receives Bill, OCR Secures $2.175 Million Fine

Sentara Hospitals in Virginia and North Carolina agreed to take corrective actions and pay $2.175 million to settle potential HIPAA violations stemming from a complaint alleging the organization sent a bill to an individual containing another patient's PHI.[1] OCR determined Sentara mailed 577 patients' PHI to wrong addresses. Sentara reported the incident as a breach affecting only eight people because they concluded (incorrectly) that unless the disclosure included patient diagnosis, treatment information, or other medical information, no reportable breach of PHI had occurred. "Sentara persisted in its refusal to properly report the breach even after being explicitly advised of their duty to do so by OCR," the office reports. OCR also determined Sentara failed to put a business associate agreement in place with another company.[1]

Matthew R. Fisher, JD, partner with Mirick O'Connell in Worcester, MA, says the easy lesson is not to fight with

OCR over interpretation of the regulations implementing HIPAA. Some portions of the regulations may be subject to reasonably different interpretations. However, if OCR says it believes a bigger breach than reported occurred, pushing back is destined to fail.

The common thread that runs through breach-related settlements is the requirement for companies to develop policies and procedures to comply with applicable notification regulations, says **Eric B. Stern**, JD, partner with Kaufman Dolowich & Voluck in Woodbury, NY. In fact, he says, most of the "Corrective Action Obligations" section of the "Corrective Action Plan" relates to forming and distributing of such policies and procedures.

As new privacy laws and regulations are put forth on both the state and federal levels, Stern says every covered entity should work with competent counsel to develop policies and procedures for breach preparedness, avoidance, and response that is compliant with applicable laws and regulations; conduct a bi-annual audit of the policies and procedures to ensure compliance; and follow those policies and procedures to prevent a breach and in response to one. Despite healthcare providers having to comply with HIPAA since 1996, they still continue to violate the law by failing to properly report breaches and by failing to put business associate agreements (BAA) in place, says **Sara H. Jodka**, JD, an attorney with Dickinson Wright in Columbus, OH. "These issues are HIPAA-compliance 101, yet healthcare providers are still messing these requirements up. It would be different if we were dealing with new technology issues, such as ransomware attacks or a new type of code-corrupted ERM databases, but this is not that," Jodka says. "This is failing to neglect simple, routine HIPAA compliance requirements."

Healthcare providers still have to sweat the small stuff. "Firewalls and state-of-the-art technology are critical for HIPAA compliance, but those things are just as important as proper reporting and having proper BAAs in place," she says.

Marissa G. Weitzner, JD, senior counsel in the Houston office of Clark Hill, noted there were three seven-figure fines levied in 2019 related to HIPAA violations. This is a sign OCR will continue its robust HIPAA enforcement.

"Sentara's self-reporting was incorrect, and its insistence on an inappropriate definition of what constitutes PHI increased its liability," she observes. "Had Sentara appropriately entered into a BAA with its parent entity, or appropriately self-reported the breach, it is unlikely it would have incurred liability for the business associate matter."

Matt Frederiksen-England, CHC, CHPR, CHRC, faculty member at Walden University in Minneapolis, says there are several action items these settlements might prompt for compliance:

• Review organizational policies to ensure they detail the patient's right to access medical records within 30 days of the request and the patient's right to request their medical records in a specific format, either paper or electronic;

• When releasing information, verify employees are following a practice that demonstrates compliance with the individual's right to access requirements;

• Ensure breach notification policies are up to date.

Because the HIPAA Privacy Rule allows a covered entity to perform a risk assessment, it is imperative professionals develop a tool to evaluate a potential breach before assuming an event is nonreportable. According to OCR, this tool should include the following factors:

• The nature and extent of the PHI involved, including any patient identifiers or likelihood of reidentification;

• The unauthorized person who used the PHI or to whom the disclosure was made;

• Whether the PHI was viewed or acquired;

• The extent to which risk to the PHI was mitigated;

• Ensure a policy exists regarding BAAs, and a process is in place to ensure contract and capital purchases are reviewed to ensure appropriate BAAs are in place. ■

REFERENCE

1. HHS.gov. OCR secures $2.175 million HIPAA settlement after hospitals failed to properly notify HHS of a breach of unsecured protected health information, Nov. 27, 2019. Available at: http://bit.ly/2U1LeML.