HOSPITAL ACCESS MANAGEMENT™

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

INSIDE

RELIAS MEDIA

SEPTEMBER 2020 Vol. 39, No. 9; p. 65-72

Easier to Ask for Race, Ethnicity, and Language Data if Registrars Know Why

Registrars may ask patients for information about race, ethnicity, and language. But if patients ask why, registrars may not be prepared to answer that question because they do not know either.

"The more the staff know, understand, and care about it themselves, the better they'll do at explaining the data collection to patients and family members," says **David Nerenz**, PhD, director emeritus of the Center for Health Policy and Health Services Research at Henry Ford Health System in Detroit.

Many patient access departments are examining their practices for collecting race, ethnicity, and language data. "We have all been reminded of the importance of equity, given the evidence of racial and ethnic disparities in COVID incidence and mortality, and the broad discussions of racism in society and in healthcare more specifically," Nerenz observes.

Hospitals want to show care processes and outcomes are not different based on patient race or ethnicity.

"The only way to do that is to collect the data, and then stratify the whole range of hospital quality measures by race/ethnicity," Nerenz offers.

If disparities are identified, then those disparities become important targets for quality improvement initiatives. At Henry Ford Health System, "we generally collect the information at registration or at outpatient visit check-in," Nerenz reports. He says patient access should use two key documents:

- The Health Research and Educational Trust Disparities Toolkit. (Available at: https://bit.ly/3g0wx4O)
- The 2009 Institute of Medicine report: *Race, Ethnicity, and Language Data: Standardization for Health Care Quality Improvement*. (https://bit.ly/330OoVO)

"Both provide good, tangible examples of how and when to ask questions of patients," Nerenz says.

Some patients are worried the data could be used against them in some way. It is important for registrars to tell these patients, with confidence, how the data are not going to be used. "This is not about finding people with immigration or visa problems. This is not about findings ways to discriminate against people," Nerenz stresses.

The data are needed for a simple and important reason, according to Nerenz: "It's about working to achieve health

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:
(800) 688-2421
customerservice@reliasmedia.com
ReliasMedia.com

AUTHOR: Stacey Kusterbeck
EDITOR: Jonathan Springston
EDITOR: Jason Schneider
EDITORIAL GROUP MANAGER: Leslie Coplin

and healthcare equity." Consistent data collection allows the hospital to compare itself to other hospitals, in terms of race, ethnicity, and language. Accuracy is important, but most uses of the data can tolerate a small amount of error or inaccuracy.

"Getting perfect data is the ideal goal. But getting good data is better than not getting any data at all," Nerenz suggests.

Which specific ethnicities and languages are offered as likely options varies by the hospital's geographic location. "Hawaii is not the same as Montana in this regard," Nerenz notes.

Standardized scripting is recommended to explain the reasons for collecting these data. "Hospitals using these approaches have had success in gathering data, and then in using the data to work to reduce or eliminate disparities in care," Nerenz says.

Without good data on race, ethnicity, and language, it is impossible to analyze differences in healthcare outcomes. "There is no other way to get these data than by getting it from patients themselves," says **Tara Oakman**, a senior program officer with the Robert Wood Johnson Foundation in Princeton, NJ.

Asking sensitive questions requires a certain amount of skill and expertise. "It is very important that the patient be asked for this information in a way that builds trust," Oakman stresses.

Registrars should make eye contact, and give clear answers on how the information will be used. "In the current environment, where there is a lot of mistrust of institutions, patients may be unwilling to provide it in a way that is useful or accurate," Oakman cautions.

Victoria Warren-Mears, PhD, RDN, FAND, director of the Northwest Tribal Epidemiology Center in Portland, OR, recommends these processes:

• **Design tools and processes that allow patients to accurately self-report their identity.** "Allow patients to report their racial and ethnic background separately, with the option of choosing multiple races," Warren-Mears says.

• **Develop written policies for race/ethnicity/language data collection.** "These policies should clearly state the reasons why this information is being collected, and how the information will be used," Warren-Mears explains.

• **Provide adequate and regular training on the importance of collecting the data.** This is particularly important if the information is collected verbally. "Training should provide staff with scripts and opportunities for practice," Warren-Mears adds.

Some registrars make assumptions about an individual's racial/ethnic background. For example, in the Pacific Northwest, American Indian last names are confused with similar family names for those of white ancestry. In the Southwest, individuals may be misclassified as Hispanic, when in fact they are American Indian.

"Hospitals can address these concerns by investing in staff training, developing educational materials, and working to support a culture of inclusion for patients and staff," Warren-Mears offers.

Some registration systems include hard stops that will not allow registrars to continue without completing the data field. "If staff are not trained to collect the data, it's easy to click 'other' or 'unknown' to complete the registration," says **Romana Hasnain-Wynia**, MS, PhD, chief research officer at Denver Health.

Registrars are more likely to do this if they think the question is just one more administrative burden. "It's not supposed to be just 'The feds require that we record this.' It's being

on the front lines of reducing known disparities," says Hasnain-Wynia, former director of the Addressing Disparities program at the Patient-Centered Outcomes Research Institute.

Most hospitals will say they are mission-driven. "But can they say that as part of our core mission, we are going to be on the front lines of reducing the known disparities?" Hasnain-Wynia asks.

Seeing this bigger picture motivates registrars to do more than just complete a data field. "What we do in our jobs differs. But patient registration staff is an important partner in this."

Even so, some registrars dread confrontations over why they are asking about race. Hasnain-Wynia estimates this probably happens only about 3% of the time. If and when it does, scripting can provide registrars with a good response, such as, "Thank you very much. We appreciate that you don't want to answer the question."

In the vast majority of cases, the registrar completes the registration without incident. Yet as with any initiative, to get results, patient access leadership must address concerns of frontline staff. "Just saying, 'Collect the data' — we know that doesn't work," Hasnain-Wynia adds. ■

Tips to Help Collect Race, Ethnicity, and Language Data

Obtaining race, ethnicity, and language data at registration is for patients' benefit. It is a way to identify the population the hospital serves, compare outcomes, and find areas that need improvement.

"Most importantly, we ask because we care. We strive to provide the same level of care for all of our patients," says **Pam Masters**, MSHS, senior director of the scheduling center at Cincinnati (OH) Children's Hospital Medical Center. Here, patient access leaders at diverse hospitals share their best processes:

At Cincinnati Children's, "training is the most important tool," Masters says. Schedulers and registrars are informed on how the data are used to improve care. Making it a part of their normal routine is a clear expectation. "We do have a robust auditing process for scheduling and registration staff, and these data fields are included," Masters notes.

Registrars do receive occasional push-back from parents. "That's definitely the No. 1 challenge," Masters reports.

Staff engage in mock calls and role-playing exercises to respond in a clear and compassionate way. Either of these sample responses are used if families seem apprehensive about answering:

- "We pride ourselves at Cincinnati Children's on being the leader in child healthcare. We collect information from all patients on race, ethnicity, and language. Knowing more about patients' race and ethnic backgrounds, we are able to know the health risks patients may have and provide the healthcare they need."
- "We collect race, ethnicity, and language data to make sure all our patients receive the same level of care. These data help us to provide services such as interpreters. Some diseases and conditions are race-specific. These data provide valuable information for our healthcare providers to use in diagnosis and treatment."

At Cooper University Hospital in Camden, NJ, trainers hold sessions for registrars specifically on why race and ethnicity data are needed. "In addition, they are familiarized with how they could answer patients' questions, should the need arise," says **Pamela Konowall**, CHAM, assistant director of healthcare access.

Trainers inform participants that New Jersey ranks as one of the most ethnically diverse states in the country. "Registrars are reminded that it is their responsibility to collect accurate registration information," Konowall reports. This includes race and ethnicity data. "It's explained to the registrars that the information that is collected is considered meaningful information that is used by clinicians to assist in determining patients' risks for contracting illness and the best treatment," Konowall explains.

The data also are used to assist hospitals across the state in giving all patients high-quality care. "The importance of collecting this information was reiterated," Konowall says.

The data collected are the only way to identify the patient population that is treated. In turn, the data can measure quality, safety, and discrepancies in care. "This information is clear documentation of patient populations that are treated in the facility," Konowall says.

Trainers review how to ask the questions, and how to explain why the information is needed "The registrars are able to respond with ease," Konowall notes.

Registrars state, "We use the data to identify differences that may exist for quality of care, identify patients' risks for developing health conditions, and create programs and services to provide quality care."

At Augusta Health in Fishersville, VA, registrars ask, "Which best describes you as a person?" Then, registrars offer a list of options, and enter the patient's response.

"The vast majority of patients will easily provide answers by asking in this manner," says **Dolly Ellis**, director of patient access.

Some people do ask why the information is needed. Registrars simply explain that it is used for safety and quality purposes.

"Once we've stated the reason, it is rare for a patient to pursue additional questions," Ellis reports.

At Rochester (NY) Regional Health System, registrars print a form with a checklist so patients can self-report the information. "We collect the information to plan quality improvement initiatives, to better understand patient demographics, and ensure adequate interpreter services," says **Tiffanie Ball**, patient access director.

Staff use this scripting: "Our goal is to ensure all patients receive the best care possible. We would like you to tell us your racial/ethnic background and preferred language so we can meet your needs." "This can often be a sensitive subject," Ball acknowledges. "The first thing we address with our staff is challenging assumptions."

Many registrars believe they can answer the questions themselves, based on patients' appearance. The patient access department found a creative way to dispel this misconception.

During a recent in-service, staff viewed photos of 10 different patients. Managers asked them to identify the race and ethnicity of each person.

"Many were shocked when they were wrong," Ball says. "This exercise really helped iterate the importance in self-reporting." ■

Patient Access Tracks Metrics Regarding Financial Experience

The patient's financial experience has become extremely important to patient access departments, but data are not easy to collect.

Hospitals usually do not include questions about financial practice in satisfaction surveys. "This is due to the many delays it can take with insurance to process and for them to get a bill," says **Stephanie Benintendi**, MBA, CHAM, director of finance and operations at Children's Hospital Colorado.

Today, some departments are using a "financially cleared" key performance indicator (KPI) from the National Association of Healthcare Access Management (NAHAM)'s AccessKeys. "Just having one component in place and doing it well does not generally speak to the overall effectiveness of the program," notes Benintendi, chair of NAHAM's Industry Standards Committee.

"Financially cleared" means preregistration demographics are collected and verified, insurance is verified and active, all necessary authorizations are obtained, all medical necessity checks are in place, a price estimate is completed, and the patient is screened for additional assistance. For those who do not meet the criteria, arrangements are made for collections or to set up a payment plan.

One obvious challenge with financial clearance is it covers so many processes — scheduling all the way to financial assistance. "If there is a centralized department, where all of this reports to one central manager/director team, then it all is encompassed into patient access," Benintendi notes.

Many hospitals operate with decentralized processes. The scheduling team reports to managers in each clinical area. Preregistration reports to a patient access manager. Insurance verification reports to a financial service manager. "This makes it hard to hold other departments accountable to the activities you need them to perform in order to hit the goal," Benintendi observes.

Even departments that have worked hard to improve financial practices find room for improvement. "A common gap we find is that many organizations have not adopted estimates," Benintendi reports. Providing an estimate, and collecting based on it, allows the organization to score higher on the preregistration process. For many, the problem is consistency. Some departments give estimates only for high-dollar diagnostic procedures. Most hospitals are not offering estimates for surgical procedures or for emergency department visits.

"It's harder to get all of the CPTs loaded that make up the charges for the contract manager to evaluate for any stop losses or carve outs," Benintendi says.

NAHAM also created a new "transparency" domain. This groups together the relevant KPIs (consistently giving estimates, the estimate accuracy rate, and identifying financial responsibility early). Another related KPI tracks the conversion rate of uninsured patients to a financial assistance plan. "This ensures you are following 501(r) requirements before sending a patient to bad debt for their portion," Benintendi says.

Some states also require surprise billing disclosures to be obtained

from each patient. "This ensures they understand their out-of-network benefits, and what options they have, before they even incur the expense," Benintendi explains.

Patients want confidence that estimates are correct. "It creates trust that the hospital cares about their financial health as well as their physical health," Benintendi offers.

Hospitals that outperform other similar facilities have something to point to. "That is something to totally capitalize on and market as a differentiator," Benintendi suggests.

Many hospitals start with a "good" rating from the AccessKeys. If so, patient access can use this rating to make a business case for needing upgraded technology to receive a "better" or "best" rating.

"A technology capital ask from a non-revenue-generating department is one of the hardest uphill battles to make with IT and senior executives," Benintendi laments. Creating a dashboard of the AccessKeys benchmarks, and where the department stands currently, is a powerful tool. "This is a great visual for senior leaders to discuss at monthly or quarterly revenue cycle steering committee meetings," Benintendi says.

Accounts can be financially cleared in many ways, with point-of-service collections, payment plans, or financial assistance. "Each area of patient access contributes to the success of a financially cleared patient," says **Melissa A. Salyer**, CRCR, a founding member of NAHAM's Industry Standards Committee and vice president of implementation at AccuReg.

The hardest part, says Salyer, is "determining the source of truth for the data." Data can come from registration systems, billing systems, or various third-party sources. Once that is sorted out, patient access sees significant benefits to resolving accounts on the front end. Patients avoid accounts going to collection. Sometimes, patients avoid catastrophic medical bills.

"Imagine the positive experience for a patient who qualifies for a hospital financial assistance program being identified in advance, and that assistance being given before the bill drops," Salyer offers.

For hospitals, there is less money to collect, fewer A/R days, and less aged A/R and bad debt. "Leading practice includes having the financial conversation early in the preregistration process for scheduled visits," Salyer says.

Patients expect to be able to electronically access all kinds of healthcare information, even price estimates. Often, patients cannot factor in their own insurance coverage to price estimates. "This would be an opportunity for the hospital to add technology to provide that solution," Salyer suggests.

Tracking transparency metrics "allows hospitals to identify gaps in internal processes, improve those processes, and possibly gain a dedicated patient to their brand," Salyer adds. ■

Department Cuts Wait Times to Under 2 Minutes — With Fewer Registration Errors

At Goshen (IN) Health, metrics have given the patient access department a much broader perspective on how well it is performing.

"It provides a benchmark of our performance that is a national standard, and not just based on our own performance," says Patient Access Director **Sue Plank**, LCSW, CHAM.

Using the National Association of Healthcare Access Management AccessKeys, Plank's department has made great progress in two areas:

• **Average wait times have decreased from 11 minutes to two minutes.** The department had been trying to address wait times for many years. It created its own metrics to measure improvement.

Before, registration wait times were measured manually at check-in. "We had software capabilities that we had never implemented," Plank notes.

Finally, the department decided to use that software to track wait times electronically. Specifically, the software uses AccessKeys for daily reporting.

Today, Plank's department can collect the benchmarks to measure against, and the same is true for registrars. Employees can see their own registration times and their colleagues' times.

"This inspired motivation for improvement, particularly in those of us with a little competitive spirit," Plank reports.

When the COVID-19 pandemic began, Plank's department made significant changes to the registration process. All outpatient registrations were moved to the main lobby. Walk-ins were asked to schedule appointments in advance. "Reduced volume allowed us to trial some new processes and technology," Plank says.

By reducing walk-ins and increasing preregistered accounts, registration times decreased sharply. When elective procedures returned, all registrations still were handled in the main lobby. Registrations per week averaged 600 previously; now, that number is more

than 800 — all while using the same registration full-time equivalent.

"But more dramatic was the number of patients who waited more than 10 minutes," Plank says. Out of 600 patients in March, 212 waited more than 10 minutes. As of July, only 52 of 857 patients waited more than 10 minutes.

Patients are noticing. Some have commented on the short wait times. "We have many days where the number of patients waiting more than 10 minutes is in single digits," Plank adds.

• The department greatly improved registration accuracy. "Colleagues wanted to do good work, but didn't have tools in place to measure their performance," Plank observes.

The department created ways to honestly look at accuracy rates. "We didn't defend or deny our mistakes," Plank says.

The emphasis was on how inaccurate work created rework for other areas of the revenue cycle. "We began to realize that there was no registration standard across the health system," Plank recalls. Each registration area was developing its own standard.

First, the department implemented software that would audit every account each time. Registrars can see their errors, and are held accountable for making corrections without waiting for someone to tell them a mistake was made.

"This allowed us to determine whether errors were contained to individuals, or whether it was systemic," Plank says.

Staff also look at their resolution rate. This tells them how many errors are going uncorrected.

"Colleagues may make few errors. But if those errors go uncorrected, they can still have a significant impact on denial rates," Plank adds. ■

Prior Auths Continue Delaying Care; Serious Adverse Events Reported

Faxing (and refaxing) prior authorization requests, and spending hours on hold with payer representatives trying to get answers, wreaks havoc with productivity in most patient access departments. Evidence shows it also hurts patients' clinical outcomes.

About one-quarter of physicians say the prior authorization process resulted in a serious adverse event for a patient, according to a survey of 1,000 physicians conducted by the American Medical Association (AMA).[1]

"It is surprising and highly disappointing that two and a half years after a landmark consensus statement signaled insurers were open to reforming the arduous prior authorization process, little progress has been made," AMA President **Susan R. Bailey**, MD, says.[2]

Physicians still face an overwhelming volume of prior authorizations, confusing requirements, and manual processes, the survey revealed. "It is hard to see how prior authorization is saving health plans money," Bailey says. Other key findings:

• A total of 16% of physicians surveyed said the process led to a patient winding up hospitalized.

• Most physicians (74%) said prior authorization delays resulted in some patients abandoning the recommended treatment plan.

• Most (86%) said the prior authorization burden has only grown worse over the past five years.

• Phone and fax remain the most commonly used methods for prior authorizations.

• Most physicians (67%) reported difficulty in finding out whether a prescription or service needs prior authorization.

Patients are going to start advocating for prior authorization reform, Bailey predicts. "More and more people struggle with care delays. We see this in the many heart-wrenching patient stories submitted on the AMA's 'Fix Prior Auth' grassroots website."

Thanks to the COVID-19 pandemic, patient access staff are dealing with tighter timeframes for authorizations. People put off care for months; today, many want to make up for lost time — and do not want to wait longer just because a health plan will not give an answer on authorization. "We have a lot of patients coming for appointments now, but we have less lead time. We are getting less time to do everything we need to do," says **Michael Sciarabba**, CHAM, MPH, director of patient access services at UChicago Medicine.

Payers normally take a week or two to give an answer on authorization. Now, patients want appointments on short notice. "Payers haven't adjusted to that. They still have their rules in place," Sciarabba observes.

In response, Sciarabba's department revamped its insurance verification process. Any appointment less than three days out is considered an "add-on." A different process is used for those appointments. "If we put them through our normal workflow process, we probably wouldn't get the auth in time," Sciarabba explains.

The real problem, according to Sciarabba, is that "the payers aren't

changing their requirements, despite the fact that the whole world has changed."

If someone makes an appointment for a procedure or test that needs an authorization, staff submit the request that same day. Someone follows up the next day. The department has enjoyed some success in securing quicker authorizations using this method.

"We are submitting the auths on the date of service, or the day before the service, and found a lot of them are being approved," Sciarabba shares. This saves appointments from cancelation. The downside is that it is a labor-intensive process for patient access. "We are having one or two people focus just on the concurrent auths," Sciarabba says. Recently, a patient was happy to make a long-awaited appointment five days out. Staff immediately set to work on securing authorization.

However, the day before the appointment, there still was no answer from the health plan. Staff had no choice but to call the patient (who had already taken a day off work for the following day's appointment) and ask him to reschedule the visit.

Registrars went into high gear, doing everything possible to obtain a payer response. First, staff made multiple phone calls asking for the request to be escalated to a supervisor. Next, staff talked to a care management nurse, asking her to authorize the service. "We basically said, 'Your patient and our patient has been waiting three months for care. He is unhappy, and it could be unsafe,'" Sciarabba says.

Finally, the nurse authorized the service. Patient access brought the man in for an appointment the following day. "It took a lot of extra work," Sciarabba says. "But we got it." ■

REFERENCES

1. American Medical Association. 2019 AMA prior authorization physician survey. https://bit.ly/2Xf2Eqj
2. American Medical Association. Consensus statement on improving the prior authorization process. https://bit.ly/2CPkAk9

Patient Identification Issues Start at Registration

Most patients will remember bedside nurses verifying their name and date of birth many times during their hospital stay. Few realize it was registrars who started the patient identification process.

"It is important that registration staff recognize the impact of misidentified registrations," says **Julie Pursley Dooling**, MSHI, RHIA, CHDA, FAHIMA.

Duplicate medical records can cause medical mistakes, problems with reimbursement, and even carry legal ramifications.

"Patient access plays a critical role in identifying and matching patients to their health record," says Dooling, director of health information management (HIM) practice excellence with the American Health Information Management Association.

It all starts with collecting accurate patient demographic information. "If a first, last, or middle name is misspelled, which happens because we are all human, there is a possibility of not finding the patient's previous records in the system," Dooling explains.

This creates a dangerous problem: a duplicate patient record that is separate from the rest of the patient's clinical information. To prevent data entry errors, Dooling recommends using a third party augmented data source to confirm names, addresses, and phone numbers.

She also suggests ongoing training for employees on patient identification processes. New hires probably have no idea the demographic information they input affects patient safety. There are several questions a registrar could ask to ensure he or she has identified the correct person:

- Have you ever received care from this facility?
- Is there a certain preferred nickname everyone calls you?
- How do you spell your last name, first name, and middle name?

• What is your legal name on your birth certificate or other legal documents?

• Do I have this punctuation correct in your name?

Patient access uses data in the master patient index to search for patients they are registering. HIM staff are the ones who manage these data. "Identifying gaps in policies and procedures in both areas of practice can solve issues that may lead to errors," Dooling says.

Part of the issue is registrars do not realize how dangerous a duplicate medical record can be. "Educating users on the dangers of duplicate medical records is a must," says **Ryan Mills**, MBA, regional director of access services at Baptist Health Hospital in Lexington, KY.

To really bring this point home, Mills asks registrars to consider a patient with a drug allergy brought to the hospital by ambulance, who arrives unresponsive.

"If no one is with the patient to confirm demographics, this could easily result in a duplicate record," Mills notes.

In this situation, clinicians could end up giving the patient the drug to which he or she is allergic. "You can never trust when a patient states they have not been to your facility," Mills adds.

Sometimes, people came for a diagnostic test or office visit years ago, and do not recall it. Other times, people do not realize they actually were treated within the health system because they were seen at a different location. To cover all these possibilities, registrars conduct multiple searches for the patient before creating a new medical record. They use this process:

• First, registrars search by the patients' Social Security number, if the patient agrees to provide it. "This is a unique value that no one else has," Mills says. There may be two patients named John Smith with the same date of birth, but they will not share the same Social Security number.

• If the initial search returns no results, the second search uses the patient's first and last name, along with date of birth. "This search will help to capture those individuals who wish not to provide a Social Security number," Mills explains.

• If there are no results again, registrars perform a final search of the person's first and last name.

If there are matches, the registrar verifies it is really the same person by gathering some additional demographic information. This search identifies people who are in the system, but are listed under an incorrect name or date of birth.

"Only after these three searches is a new medical record to be created," Mills says.

The department has reduced the number of duplicate records by carefully following these processes. When it does happen, immediate action is taken.

"We use the opportunity to re-educate that team member, sharing the associated dangers," Mills adds. ■

COMING IN FUTURE MONTHS

- Out-of-network status is missed if patient self-schedules
- Claims denied because service is excluded from coverage
- Hospitals marketing consumer-friendly billing practices
- Price estimates so accurate they can be guaranteed

HOSPITAL ACCESS MANAGEMENT™

HIPAA REGULATORY ALERT

CUTTING-EDGE INFORMATION ON PRIVACY REGULATIONS

HIPAA Compliance a Concern as Working from Home Becomes Norm

Working from home is the new normal and will be for many healthcare employees for a while, so adjustments are necessary to maintain compliance with HIPAA. Protected health information must be managed properly whether the employee is in the healthcare facility or at home.

Most healthcare providers should have crafted compliance programs for remote employees before the advent of the COVID-19 pandemic. Certainly, the pandemic has pushed the urgency of such plans to the forefront, says **Richard J. Tarpey**, PhD, assistant professor in the Jones College of Business at Middle Tennessee State University.

"In my prior practitioner healthcare career and leader of Sarbanes-Oxley and HIPAA compliance programs in the past, I can say that compliance is not flexible based on the location of the workforce. It is absolutely reasonable to expect the same level of security for remote workers as is in place for employees on company property," he says. "There are several examples in the last few years of healthcare providers being held financially accountable due to the loss of PHI [protected health information] data by remote employees."

The first step is for companies to completely understand which employees have remote access, Tarpey says. Existing remote access should be reviewed and reaffirmed to those employees with valid business justification. Companies should require, and employees should be willing to sign or reaffirm, confidentiality and HIPAA compliance documents. "It is a good idea to refresh the employee obligations in the employees' minds at this time," Tarpey says.

Compliance documents should highlight policies prohibiting using company-issued devices for non-company-related work, as well as preventing non-employees from using company-issued devices or using any personal devices that connect to company networks. Also underscore the importance of properly storing PHI-sensitive printed documents, and logging off all systems after finishing work.

Policies should clearly state the consequences of violation, Tarpey says. It also is a good idea to provide refresher information for employees on printing documents at home that contain PHI information. If reasonable, companies can consider providing HIPAA-compliant shredders for employees' use at home. Alternatively, companies can create structured processes for employees to drop off printed documents no longer needed at the company location via social distancing-safe processes.

On the technology side, companies should require remote employees to use a VPN to access company infrastructure when working remotely. Also, ensure the encryption of home wireless router traffic with secure (not default) passwords. Companies can best control access by issuing remote employees who access PHI a company-owned device that is encrypted and password-protected.

"The best [tactics] are to have strong remote work and data access policies, signed HIPAA compliance documentation for each remote access worker, and robust device management policies for any device connecting to the company network," Tarpey says. "While risk mitigation of a PHI data breach can never eliminate the risk with remote employees, the key determining accountability factor in the eyes of [Health and Human Services] is how well the company has managed system access, data access, system-connected devices, encryption, and employee policies."

The COVID-19 pandemic has prompted healthcare providers to ramp up work-from-home programs for non-clinical staff, often for the first time, and certainly at a scale not seen before, says **Rich Temple**, vice president and chief information officer at Deborah Heart and Lung Center in Browns Mills, NJ. "I think all providers need to operate from the premise that the level of cybersecurity protection

provided in a work-from-home environment can be no less than what it would be in an on-site working environment," Temple says. "The consequences of data breaches and security lapses, if anything, are greater in a work-from-home environment, since the control of who is seeing what is reduced when working in a household environment. The negative consequences of breaches are still the same, regardless of where the breach originated."

With a VPN, users go through the same, secure tunnel that allows IT teams to know exactly what volume of users are on what systems at different times. IT teams can allow "one-stop shopping" reporting on security red-flags, such as multiple failed log-in attempts or unusual access patterns (e.g., logging into systems at unusual days or times for particular users), Temple notes. The single point of entry also facilitates appropriate access to only the systems an individual needs to perform his or her job.

Another highly desirable protection to put in place, if at all possible, is two-factor authentication (2FA), Temple says. Instituting 2FA largely mitigates the risk of someone using a shared or otherwise purloined password to gain access to a system to which they are not entitled.

"The virtual desktop infrastructure [VDI] environment we have rolled out here at Deborah Heart and Lung allows us to greatly reduce our exposure to any malware issues that may reside on a user's home computer. [It] also minimizes the potential for data loss, [losing] electronic protected health information [ePHI], or [misplacing] other proprietary data assets," Temple says. "When a user logs into our environment, they are presented with a containerized, segregated virtual desktop ... our environment does not allow any sharing of programs or data between the home computer and the user's isolated VDI session."

The worst-case scenario is anything installed on the virtual desktop is destroyed when the virtual desktop logs itself off after a prescribed period and will not cross over and pose a risk to other users' virtual desktops, Temple explains.

Another issue is the "paper" component of individuals' job duties, Temple says. In an office, paper containing PHI can be stored in a desk at a cubicle. With good "HIPAA hygiene," one can protect this information from unauthorized eyes. However, with employees working from home, provider organizations lose those structural safeguards. It becomes much harder to ensure family members or others do not see PHI lying on a coffee table.

Printing PHI should be sharply restricted, if not prohibited altogether, for employees working at home, says **Janet Hunt**, senior director of IT user support at Apria Healthcare, a provider of home respiratory services and medical equipment based in Lake Forest, CA. Apria employees have worked remotely to an extensive degree long before COVID-19. Hunt says restrictions on printing PHI are a necessary part of HIPAA compliance.

"It's impossible to know where that PHI goes once it's printed on paper. We can't have it sitting around someone's home for just anyone to come by and see," she says. "With some reasonable precautions, I think employees can be just as HIPAA-compliant working from home as they are in the workplace."

The printing issue is an example of how employees can be tripped up by the peculiarities of working at home, says **Elizabeth Litten**, JD, partner and HIPAA privacy and security officer with Fox Rothschild in Princeton, NJ. "I know of a physician who was staying at her parents' house and had to submit a lab report. She did it from her own laptop just as a quick way to transmit it. Unbeknownst to her, it also printed to the printer in her old bedroom," Litten says. "She didn't realize that for a long time. That PHI was sitting there for her parents and anyone else who happened to be there to see it. There are more opportunities for inadvertent breaches when you're working from home, even if you're trying to do it properly, because someone can just walk by and see what's on your screen or overhear what you're talking about."

Implementing good tools for remote access and ensuring verification of the user are the keys to HIPAA compliance at home, says **Matthew R. Fisher**, JD, partner with Mirick O'Connell in Worcester, MA.

"To some degree, the HIPAA considerations when having a workforce operating from their homes as opposed to the office do not introduce new concepts. The basics of ensuring that workstations and network access remain secure should be paramount," he says. "On the whole, the policies should focus on maintaining the integrity of the system and keeping data as secure as possible. For example, allowing remote access to the entire system with no more than a username and password would not be advisable. Instead, some form of multifactor authentication or other mechanisms for vetting a request for access should be implemented."

On top of system-based tools, sending reminders to individuals working remotely of how to secure work areas and data can be beneficial, he says. Reminders can take the form of teachable moments or short pieces on how to apply office-based procedures to a home environment.

IT staff will play a large role in ensuring HIPAA compliance for

remote employees, says **Timothy E. Monaghan**, JD, partner with Shutts & Bowen in West Palm Beach, FL. He says the question should be: Are our communications with employees working from home protected to the same degree as communications between our employees when working from our facilities and offices?

If the issue is communication between the healthcare entity and persons not on its payroll (such as outside counsel or consultants), the security issue is not new to COVID-19. Perhaps COVID-19 is causing the entity to review security issues in general, Monaghan offers. If this is the case, the pandemic may be uncovering issues that have been present for some time. If so, the entity would be justified in asking outside parties with whom it conducts business to demonstrate compliance with privacy and security regulations.

Another solution is to ensure sensitive information is not shared with outside parties who may not need it for their work.

"If I anticipate receiving PHI from a client, I make sure that I have a HIPAA-compliant Business Associate Agreement in place before I receive the PHI. I work with our IT folks to arrange for secure transmission and storage," Monaghan says. "Most of the time, however, I can do my work without personally identifying information. I simply advise the client to exclude that information from any communications with me."

As always, organizations should be careful to ensure PHI is shared on a "need to know" basis. This is true whether the person receiving it is working in the office or at home, Monaghan says.

"A number of HIPAA requirements have been waived. I believe this is in general recognition of the fact that we are in extraordinary times. It is more important now to keep healthcare organizations running as smoothly as possible and to simply make sure we save lives," Monaghan says. "It probably is not reasonable to expect the same level of security at home right now, but ... we should make sure that our pre-COVID practices were in order and that exceptions to full compliance are reasonable under the circumstances. In other words, we can't assume that all transgressions will be forgiven because we are in this crisis."

Covered entities should ensure HIPAA compliance the same way they did pre-pandemic: by analyzing the risks and adopting safeguards that minimize those risks, says **Jeffrey Drummond**, JD, an attorney with Jackson Walker in Dallas. There were many healthcare providers and other health industry businesses that already worked remotely or allowed employees to telecommute while maintaining HIPAA compliance.

While each business will face its own peculiar issues, some risks expected in a work-from-home situation include data transmission security, data storage security, and person/entity/device authentication, Drummond notes. However, there are readily available safeguards for each new risk.

"It's always a good idea to limit employee access to information needed for the job. Given the potential increased risk of working from home, covered entities and business associates should readdress employee access and limit wherever possible," he says. "However, a healthcare provider should not impose any data access limitations that will impact the quality of care."

HIPAA always requires taking reasonable steps to ensure the security of protected health information. Changes in work environment do not change the expected level of security, Drummond says. What is reasonable in an emergency situation may be unreasonable in a time of calm and normalcy.

"The question in current COVID-affected times is what level of security may be reasonably obtained, given the current situation? A VPN is not as secure as a closed-access system. In that respect, working from home is going to have a lower level of security," Drummond says. "However, during a time of government-mandated work-from-home orders, that 'lower' level of security might be just as reasonable — HIPAA-compliant — as the higher level during non-pandemic times."

New approaches leveraging machine learning-based data governance enable institutions to continually monitor their data, receive notifications when a compliance risk emerges, and automate its remediation, according to **Alok Tayi**, vice president of life sciences at Egnyte, a company in Mountain View, CA, that provides data security services

"Among our customers, the key risks that have emerged involve training, data exposure, and moving data between applications. To enable learning, we have seen many companies implement distributed training tools and screen sharing to share best practices," he says. "Two [tactics] to tackle data exposure are to centralize data in what is called a 'single source of truth' and apply machine learning to see when sensitive data is exposed. Native integrations between your data repository and applications facilitate a single area of control."

Considering the dynamic effect of COVID-19, transmitting data to employees working at home may be the wrong framework, Tayi says. Instead, it may be appropriate to maintain

a central, unified database to which access is provisioned. This approach facilitates a strong security envelope around the data, but affords seamless access if permitted.

"It is possible for data to be as secure in a work-from-home model as in an office-driven one. Doing so requires the proper technologies be implemented to ensure safe and secure access," Tayi says. "Approaches like machine learning-based data governance, centralized repository models, and single sign-on enable personnel and patients to have comfort and confidence around the security of their data."

Many HIPAA threats come down to inappropriate access to patient data outside the intended context. This fundamental risk to PHI data is no different in a remote work environment than in a physical office, says **Paul Trulove**, chief product officer with SailPoint, a company based in Austin, TX, that provides data security services.

"Healthcare employees should be following the same IT security best practices as they would in the office to minimize the risk of a potential data breach," he says. "Healthcare organizations can enhance their ability to protect PHI in a remote working environment by focusing on two key areas. First, ensure workers accessing PHI are connecting to a secure network when they access internal systems that have patient data. Second, make sure they are not transmitting PHI to personal devices or personal email accounts."

Employees should use corporate-owned devices and apps sanctioned only by IT, Trulove says. "Identity management is still a critical business essential as healthcare organizations continue to operate out of the home by following the same identity governance standards. To do this, they need to continually review who has access to what, and deprovision that access if it is no longer appropriate or when someone no longer works at the organization," he says. "This is critical now more than ever as people continue to be remote." ■

7 Steps to Better HIPAA Compliance at Home

Ensuring HIPAA compliance with employees working from home will require a systematic approach. **Robert K. Neiman**, JD, principal with Much Shelist in Chicago, offers seven steps for better compliance:

• Hold a Zoom call for all employees reminding them of the company's HIPPA policy and their obligations. Ensure the policy states employees working remotely and accessing protected health information (PHI) use company-owned, encrypted, password-protected, and VPN-equipped devices. Prohibit employees from using personal devices to store or access PHI. Direct all employees accessing PHI remotely to e-sign their understanding and agreement.

• Allow employees to access only the PHI they need to handle their job. Limit access accordingly.

• Prohibit any use of the company-owned device by any third party, including friends and family.

• Make sure employees' passwords for their company device and wireless router are sufficient. They should be long and complicated enough, using a combination of letters, numbers, and symbols, to minimize the risk of hacking.

• Limit PHI printing. If any employee must print any documents containing PHI, then require he or she shred printed documents before disposing them.

• Require employees working remotely to disconnect from the company system when their work is finished for the day.

• Prohibit employees from leaving their company device in their personal vehicles at any time to avoid the risk of device theft via a break-in. ■