Hospital Access Management™

Admitting ● Reimbursement ● Regulations ● Patient Financial Services ● Communications
Guest Relations ● Billing & Collections ● Bed Control ● Discharge Planning

May 2011: Vol. 30, No. 5
Pages 49-60

IN THIS ISSUE

AHC Media

Outdated processes for patient ID must stop — Adopt new strategies

(Editor's Note: This is a two-part series on patient identification processes used by patient access departments. Inside, we cover processes used to verify a patient's identity, the expected impact of healthcare reform, and how to involve patients in the process. Next month, we'll report on new biometric technology being implemented by a growing number of hospitals.)

Identity theft and privacy protection are "the two cornerstones of today's patient access environment," according to **Robin Ten Eyck**, CHAM, director of patient access at Sound Shore Health System in New Rochelle, NY.

However, it was a challenge to create a process to comply with the Federal Trade Commission's Red Flags Rule, which requires hospital to implement programs to detect and prevent identity theft, while remaining "patient-friendly," according to **Sherri Pitkin**, associate director of patient access management at University of Iowa Hospitals and Clinics in Iowa City.

"We worked on the processes for quite some time before implementing our approach," says Pitkin. "We contacted our neighboring hospitals to discuss their thoughts and progress on procedures." Some had implemented new processes, and they shared what worked and didn't work for them, says Pitkin. Others still were in the developmental stage.

Identity theft is always a concern, says **Roxana Newton**, CHAA, patient registration and central scheduling supervisor for Porter Adventist Hospital in Denver. "Patient access is the first to greet the patient,"

EXECUTIVE SUMMARY

Patient identification processes might need to be updated to be patient-friendly and keep up with new technology. To prevent identity theft:
- Contact other hospitals to learn their approaches.
- Add scanned photo identification to the patient's medical record.
- Ask patients to tell you their demographic information.

**NOW AVAILABLE ONLINE! Go to www.ahcmedia.com/online.html.
Call (800) 688-2421 for details.**

Newton says. "It is up to us to make sure we have the correct patient and medical record number, for each and every person seen in the hospital."

This step is vital for patient care and prevents the wrong person from receiving the patient's bill, Newton says. "Our current process is very accurate to prevent identity theft. But as times change, so do thieves' strategies," Newton says. "As technology improves every year, so does our fight against identity theft."

Implementing standardized procedures regarding verification of patient identity keeps risks low, according to **Erin D. Baggett**, director of patient access for Bon Secours Richmond Health System in Mechanicsville, VA. "As the possibility of identity theft increases, so does our awareness," Baggett adds.

New processes

In the University of Iowa Hospitals and Clinics' emergency department, patient access staff check identities after medical triage, reports Pitkin.

"The IDs will soon be scanned and attached to the patient's account," she says. "The ID will be retrievable for anyone checking the patient into a clinic, admitting the patient, or registering the patient."

Staff flag the patient's account if identity theft might have occurred, adds Pitkin. "Patients with no insurance or in this country illegally have used another person's ID, insurance information or residency information," she reports.

In other cases, patients didn't want diagnostic tests in their medical record so they used a friend's ID, and patients with outstanding warrants have used an alias, says Pitkin. "We receive phone calls from patients that experienced identity theft elsewhere or believe that someone is trying to get their information, and want to be sure we have their account flagged," she adds.

The flag notifies employees to ask for additional security identifiers before checking the patient in or before giving information to the patient or patient's family, she says. "Our hospital security and our compliance department are notified of any suspicions," says Pitkin. "Security is prompted to investigate, resolve, and make further notifications to the appropriate parties."

Patient access staff at Porter Adventist scan in a copy of the patient's drivers license or photo ID card and attach it to their account, which provides a visual record of the patient, says Newton. "This is for the lifetime of the medical record number. We ask for it, if we see it has not been presented," says Newton. "With this tool, we can catch drug seekers checking in the ER using someone else's name, because now we have a picture to compare."

A "forms fast" program is being implemented to electronically capture signatures on all forms, reports Newton. "Amazingly, the pens used for this new program actually acquire the pressure used to sign by the patient!" she says.

The program automatically pulls up the forms which need to be signed, based on the type of registration and insurance information entered by the registrar, adds Newton. "If a Medicare patient

Hospital Access Management™ (ISSN 1079-0365) is published monthly by AHC Media, a division of Thompson Media Group LLC, 3525 Piedmont Road, Building Six, Suite 400, Atlanta, GA 30305. Telephone: (404) 262-7436. Periodicals Postage Paid at Atlanta, GA 30304 and at additional mailing offices.

POSTMASTER: Send address changes to Hospital Access Management™, P.O. Box 105109, Atlanta, GA 30348.

SUBSCRIBER INFORMATION

Customer Service: (800) 688-2421 or fax (800) 284-3291, (customerservice@ahcmedia.com). Hours of operation: 8:30 a.m.-6 p.m. Monday-Thursday; 8:30 a.m.-4:30 p.m. Friday.

Subscription rates: U.S.A., one year (12 issues), $399. Add $17.95 for shipping & handling. Outside U.S., add $30 per year, total prepaid in U.S. funds. Discounts are available for group subscriptions, multiple copies, site-licenses or electronic distribution. For pricing information, call Tria Kreutzer at 404-262-5482. Missing issues will be fulfilled by customer service free of charge when contacted within one month of the missing issue date. Back issues, when available, are $80 each. (GST registration number R128870672.)

Photocopying: No part of this newsletter may be reproduced in any form or incorporated into any information retrieval system without the written permission of the copyright owner. For reprint permission, please contact AHC Media. Address: P.O. Box 105109, Atlanta, GA 30348. Telephone: (800) 688-2421. World Wide Web: http://www.ahcmedia.com.

Opinions expressed are not necessarily those of this publication. Mention of products or services does not constitute endorsement. Clinical, legal, tax, and other comments are offered for general guidance only; professional counsel should be sought for specific situations.

Editor: **Stacey Kusterbeck**, (631) 425-9760.
Executive Editor: **Joy Daughtery Dickinson** (229) 551-9195 (joy.dickinson@ahcmedia.com).
Production Editor: **Neill L. Kimball.**

Copyright © 2011 by AHC Media. Hospital Access Management™ is a trademark of AHC Media. The trademark Hospital Access Management™ is used herein under license.

AHC Media

Editorial Questions
For questions or comments, call Joy Dickinson at (229) 551-9195.

is being admitted as an inpatient, the Medicare Rights form will instantly pop up to be signed," she says. "Now, nothing will ever be missed that needs to be signed." *(See related stories on health care reform, below, and involving patients in the identification process, right.)*

SOURCES

For more information on patient identification processes used by patient access departments, contact:
- **Erin D. Baggett**, Director of Patient Access, Bon Secours Richmond Health System, Mechanicsville, VA. Phone: (804) 764-6152. E-mail: Erin_baggett@bshsi.org.
- **Roxana Newton**, CHAA, Patient Access Supervisor, Porter Adventist Hospital, Denver. Phone: (303) 765-6545. Fax: (303) 778-2424. E-mail: RoxanaNewton@Centura.org.
- **Sherri Pitkin**, Associate Director, Patient Access Management, University of Iowa Hospitals and Clinics, Iowa City, IA. Phone: (319) 353-8809. E-mail: sherri-pitkin@uiowa.edu.
- **Robin Ten Eyck**, CHAM, Director of Patient Access, Sound Shore Health System, New Rochelle, NY. Phone: (914) 365-3745. Fax: (914) 633-3140. E-mail: rteneyck@sshsw.org. ■

Healthcare reform could impact patient IDs

It's not possible to gauge the full impact that the Patient Protection and Affordable Care Act (PPACA) will have on patient identification processes, says **Robin Ten Eyck**, CHAM, director of patient access at Sound Shore Health System in New Rochelle, NY.

"We do not yet know which, if any, of the currently enacted changes will materialize," she adds.

However, healthcare reform includes incentives for doctors and hospitals to adopt electronic health records. Protecting the data and securing health information will require hospitals to put technology into place to properly identify patients and reduce identity theft, Ten Eyck says.

National ID cards with magnetic strips containing the individual's health information are one possibility on the horizon, says Ten Eyck. "How much and how soon any of this becomes reality could result in vast overhauls of all our processes," she says. "For now, we trudge along, armed with electronic gizmos and relying on human intelligence to safeguard us."

Erin D. Baggett, director of patient access for Bon Secours Richmond Health System in Mechanicsville, VA, expects that the PPACA will decrease the number of patients attempting to fraudulently use the insurance of other individuals. "Healthcare reform will provide coverage to those individuals," she says.

Baggett says that an argument can be made that through the hospital's patient identification process and the PPACA, a greater population of patients will seek the coverage for which they are entitled. "As health care reform evolves, we will continue to meet the needs of protecting our patients' identities," she says. "This ensures a high level of patient care." ■

Ask patients to provide demographic information

Be secure and *patient-friendly*

Patient access staff at Porter Adventist Hospital in Denver rely on patient identifiers to prevent identity theft and ask for identification at every visit, whether it's a scheduled appointment or an ER visit, says **Roxana Newton**, CHAA, patient registration and central scheduling supervisor.

"We obtain signatures and have the patient tell us their demographic information to triple check what we have in the system," she says.

Asking the patient to verify their information is always a balancing act between patient satisfaction and security, says Newton. "Fortunately, as time has passed, the patients now expect to be asked. They have come to understand that it is for their safety," she says.

Because of Health Insurance Portability and Accountability Act (HIPAA) regulations, insurance carriers have had to assign identification numbers to patients instead of social security numbers that traditionally were used to identify patients, says **Robin Ten Eyck**, CHAM, director of patient access at Sound Shore Health System in New Rochelle, NY. "Patients are reluctant to give out their social security numbers," Ten Eyck says. "We have nothing to cross reference with, as the social security numbers are off the insurance cards."

Patient access staff can "never be too careful," says Ten Eyck, which means that patients are asked to provide picture IDs; insurance cards; and verbal confirmation of their date of birth, address, and telephone number. "It used to be that the patient

access department took basic demographic information at face value," says Ten Eyck. "Today, everything we enter is double- and triple-checked."

Discrepancies noted

Sound Shore Health Systems' patient access departments soon will implement a system that scans patient IDs into the electronic medical record for future identification of the patient, reports Ten Eyck.

Registrars cross-reference information obtained from the insurance carrier with the information given by the patient, Ten Eyck explains. Any discrepancies require further questioning by the registrar, who might ask the patient for additional forms of identification. "As appropriate, the registrar may call on their supervisor for assistance, or alert the care provider of possible aliases being used by the patient," says Ten Eyck. "If a breech occurs, security and local authorities may be called, but medical care of the individual is paramount."

At Bon Secours Richmond Health System in Mechanicsville, VA, patients are asked to bring picture identification and to verbally provide their demographic information at pre-registration. **Erin D. Baggett**, director of patient access, says, "This method of conversation prevents us from disclosing personal information."

When patients present to registration areas, staff don't perform the entire validation process, says Baggett. "We ask the patient to verbalize their full name and their date of birth," she says. "We then ask for their picture identification as part of our validation process. We convey to patients that our brief inquiry is to preserve the integrity of their identity." ■

Keep your 'stars': Offer new positions, more pay

Promote from within your department

Did you invest a lot of time and energy training a new registrar, only to have her turn around and leave your department?

"A lot of the patient access representative positions are at entry level, with commensurate salaries," says **Jeanne Day**, RHIA, CHAM, director of medical records and patient access at Greater Baltimore (MD) Medical Center. "Employees may end up transferring to different departments."

Many registration areas are open 24 hours a day, seven days a week. "I think that any area where you have these schedules along with an entry level salary, you are going to have challenges with retention," Day says.

Brenda M. Lamb, assistant director of admissions and patient access at University of California — San Diego Medical Center, says, "Being a military town, we are more likely to have turnover due to staff moving out of the area." When three management positions became available, Lamb created three lead positions for her existing patient access staff instead of recruiting outside the department. "This offered opportunities for career growth from within our department," Lamb explains. "We did not have a career ladder of sorts within the patient access department for staff promotion, which this then offered."

The strategy, says Lamb, gave her the chance to recognize several 'stars' within the department. Previously, she explains, patient access positions ranged from Level 1 to Level 3. "Over time, we've had an excellent pool of new hire candidates with years of experience," she says. As a result, all positions were transitioned to the Level 3 classification with commensurate salaries, says Lamb.

The three new positions are over inpatient admissions, emergency department registration, and financial counseling, says Lamb. Staff work in tandem with senior operations managers to ensure appropriate staffing levels and review patient accounts for accuracy, she adds. "There was a good sampling of staff interested in the few positions," says Lamb. "All were hired from within the department."

Offer pay increase

Day developed a career ladder based on staff obtaining the certified healthcare access associate (CHAA) certification, with the hospital paying for the $100 examination fee. When staff achieve the

EXECUTIVE SUMMARY

Offering new job positions and pay increases are effective ways to improve retention of patient access staff.

- Promote existing staff instead of recruiting outside the department.
- Offer pay increases for obtaining certification.
- Invite staff to lunch so you can learn their ideas for improvement.

certification, they receive a 5% pay increase, says Day.

"This is a basis of showing expertise in the field," she says. "We've had really good results with it." Previously, none of the department's 37 eligible patient access representatives had obtained the CHAA certification, says Day, but to date, 21 have done so.

"It wasn't that patient access representatives did not want to obtain the certification. I don't think they were aware it existed," says Day. "Staff are recognized for their knowledge and expertise, as well as receive a nice pay increase." *(See related stories on obtaining feedback from staff, below, and offering cash incentives, p.54.)*

SOURCES

For more information on retention of patient access staff, contact:

• **Jeanne Day**, RHIA, CHAM, Director of Medical Records & Patient Access, Greater Baltimore (MD) Medical Center. Phone: (443) 849-3554. Fax: (443) 849-8776. E-mail: JDAY@gbmc.org.

• **Brenda M. Lamb**, Assistant Director, Admissions/Patient Access, University of California -- San Diego Medical Center. Phone: (619) 543- 3489. Fax: (619) 543-7797. E-mail: blamb@ucsd.edu. ■

What can staff tell you? You'll be surprised

Ask employees for their opinions

Annual employee satisfaction surveys conducted annually by Greater Baltimore (MD) Medical Center have told **Jeanne Day**, RHIA, CHAM, director of medical records and patient access, a lot about her staff.

"We develop action plans as a result of that feedback," she says. Staff members answer 34 questions, including how well their group works as a team and whether they feel respected, she says.

Once Day gets back the results, she works with staff to develop a plan for whatever was identified as the top priority. For 2011, she says, it was the ability to work as a team with employees in clinical areas.

Patient access leaders now meet monthly with supervisors from the emergency department, obstetrics, laboratories, and other clinical areas to work on this area, says Day. "It's a work in progress. We have found it is helpful to meet face to face with these managers, so issues can be resolved in a timely manner," she says.

The department no longer has formal staff meetings, says Day, because it was just too difficult to pull staff together at the same time. Also, there is often a need to disseminate information to staff immediately, she adds. "Instead, we hold more informal meetings, which are more of a huddle with the staff," she says. "We hold these on an as-needed basis to keep them updated."

Hold group lunches

Each month, Day and the associate director of patient access invite a small group of employees to lunch. All staff members receive the opportunity to attend a lunch meeting at least once a year, she says, and they are given the chance to make specific suggestions for the department.

"There is no specific agenda. We ask them what is working well and what they feel are opportunities for improvement," says Day. "Staff have come up with a lot of ideas to make their jobs easier." For example, a label printer was moved to the Emergency Department's "Mini-Reg" workstation after staff explained it would save time and allow them to provide better service.

Day makes a point of acting on these suggestions. "I find that no matter what type of problem it is, if staff bring up something once, they feel they have met their obligation," she says. "If you don't fix it, they may never bring it up again."

If a suggestion isn't going to be possible, Day says so upfront. "It may be that staff might want to collect a copay in the emergency department before the patient sees the physician, which is against regulatory requirements," she notes. "So it is a good opportunity for staff education as well."

Day comes to the meetings with targeted questions, in the event staff aren't forthcoming with comments. "If everybody's being very quiet, I might say, 'We put up a new imaging system last month. How is that going?' Also, I try to start each meeting on a positive note."

Day asks employees, "What is the most positive thing going on with your job right now?" "It is nice to be able to go back to their supervisors and share that staff feel something is working well," she says. "At times, it feels like you're only handling problems. Everyone appreciates positive feedback."

Almost without exception, says Day, staff enjoy

being asked for their opinion. "I often get e-mails thanking me for taking the time to meet with them," she says. "Any time you are committing an hour of your time just to find out what someone's opinion is, I think most employees appreciate that." ■

Monthly POS goal of $450,000 is goal

Cash can motivate staff

At University of California — San Diego Medical Center, members of the patient access staff participate in the organization's Clinical Excellence Staff Incentive Plan, which gives them an opportunity to earn additional pay for meeting specific goals, says **Brenda M. Lamb**, assistant director of admissions and patient access.

When an individual staff member, the department, and the organization all do well in implementing strategic goals, staff become eligible to receive financial rewards, explains Lamb. "The incentive plan is based on a concept called 'gainsharing.' It is our way of acknowledging and rewarding employees who achieve their goals," Lamb says. "If we achieve our service goals, both institutional and unit-specific, at the maximum level, this year's award could be as much as $1,000 per employee."

For inpatient registration areas, for example, the service goal is based on the number of 'definitely yes' answers under the "likelihood to recommend" question on the hospital's patient satisfaction survey.

Lamb says that 25% of the award is based on the category of service. "Every employee in this organization contributes to the patient experience," she says. "We need to work as a team to ensure that customer service is given at all times."

This year, 75% of the incentive plan is based on goals developed at the department level, adds Lamb. In previous years, she says, department goals have involved customer service, courtesy of patient access staff, patient account denials specific to patient access, and improving financial viability. "It's not the same every year, which in itself is motivating," says Lamb.

Phone payments taken

This year, members of the patient access staff at University of California — San Diego are working to meet a monthly goal of $450,000 point-of-service (POS) cash collections, reports Lamb. These changes were made:

• A Financial Clearance Center was established, consisting of staff who verify insurance eligibility and benefits and document patient liability.

Members of this team contact patients to confirm their scheduled admission, says Lamb. Registrars notify the patient that their insurance has been verified, that authorization has been obtained, and that liability has been determined.

"They let the patient know they can take care of that payment now over the phone, so the patient does not have to deal with this matter on the day of their admission," says Lamb. "Their focus can be on their health needs, and not financial."

If a patient says they would rather pay on the date of service, staff document this on the patient's account, says Lamb. "It then becomes the responsibility of the front-end patient access staff to collect at the time of the patient's arrival," she says.

• Lamb receives daily reports on patients with outstanding balances.

The report gives her the amount of the deductible that already has been met and what percentage of the patient's coinsurance is the patient's responsibility as opposed to the health plan's, says Lamb.

• Refresher training was provided for staff.

This education includes detailed training on the health plan contract for each of the primary payers, says Lamb. "This increased their overall skills," she says. "Staff have more understanding of the patient's liability, including deductibles and coinsurance percentages based on expected service." ■

Those 'sharing' coverage might qualify for help

Have staff offer financial assistance

Occasionally, individuals pose as others to "share" insurance coverage with family members or friends, reports **Jane Gray**, CPA, FACHE, FHFMA, assistant vice president for the revenue cycle at the Medical Center of Central Georgia in Macon. In one such case, the medical records of a woman who delivered a full-term baby showed she had a full term delivery just three months earlier.

"She had assumed her sister's identity," explains

Gray. "We have a lot of that. People also try to share eligibility under our financial assistance program, in order to avoid paying for healthcare."

This situation happens most often in the emergency department, says Gray, due to Emergency Medical Treatment and Labor Act (EMTALA) requirements. "People are in tune with that. They know what the EMTALA laws are, and that they have a right to receive care regardless of their ability to pay," says Gray. "They are often less forthcoming in that environment."

Some of these individuals, says Gray, might be surprised to learn they are eligible for financial assistance. Gray notes that a patient making $100,000 a year could have a million dollar medical bill and quality for financial assistance. "At some point, almost everybody needs assistance," she says. "I don't know if that idea has permeated society yet, but assistance is out there for more people than you would think."

Staff now look for verbal cues that might indicate a patient's inability to pay and refer these patients to the hospital's financial assistance program, says Gray. "In the course of a conversation with a patient, they might say something that would prompt you to ask them if they would like to speak with someone about qualifying for assistance," she says.

The assistance program assesses uninsured individuals to see if they qualify for Medicaid or other programs, says Gray. "Some people know the system and work it to death. Other people don't even realize that they could qualify and are thrilled to death to get assistance," she says.

When patients utilize one of the hospital's registration kiosks, says Gray, they are asked for their date of birth and last four digits of their Social Security number. "So you get some element of protection there," says Gray. "As the patient enters payment information, there is some degree of identity validation in making sure names match and so forth." *(See related story on abuse of financial assistance, below, and use of registration kiosks, p. 56.)*

EXECUTIVE SUMMARY

Some patients who pose as others to "share" insurance coverage might be eligible for financial assistance. To avoid fraud:

- Look for cues that indicate a patient's inability to pay.
- Determine if patients receiving financial assistance have access to insurance coverage.
- Ask patients using registration kiosks for identifiers.

SOURCES

For more information on financial assistance programs and fraud prevention, contact:

• **Jane Gray**, CPA, FACHE, FHFMA, Assistant Vice President, Revenue Cycle, Medical Center of Central Georgia, Macon. Phone: (478) 633-2097. Fax: (478) 633-4071. E-mail: Gray.Jane@mccg.org. ■

Patients may abuse financial assistance

More questions are asked

At Medical College of Central Georgia in Macon, the Care Partners Program offers financial assistance for chronically ill patients in order to reduce unnecessary hospitalizations, says **Jane Gray**, CPA, FACHE, FHFMA, assistant vice president for the revenue cycle.

"A diabetic or person with high blood pressure in a lower socioeconomic environment may have a hard time complying with their plan of care," says Gray. "We try to address their financial needs so they can manage their illness. We have seen some good results with that."

When the Care Partners program was implemented, "we discovered a good bit of identity fraud as part of that process," she says. "People were sharing their eligibility cards."

It also was discovered that some people receiving financial assistance had access to insurance coverage, but they opted not to take it because they already were receiving financial help, reports Gray. "We added a new rule to say that if you have access to insurance, you are not eligible for assistance," she says.

Gray that while her department saw an increase in identity theft a few years ago, this problem has leveled off. "I think people are much more aware of the risk than they used to be," she says. "The industry in general is asking more questions and doing a better job of validation."

For face-to-face encounters, says Gray, patient access staff always ask for ID. "Of course not everybody can produce a photo ID. That tends to be a red flag," she says. "We ask if they have for any kind of ID. It may be a work badge or credit

card. We take what we can get, to give us a greater comfort level."

Over the phone, staff ask for several identifiers, says Gray. "We take great care in doing due diligence. We want to be sure we are talking to the right person who has a right to that information," she says. "If we get anything off what we have on file, we ask for another validator."

Many times, says Gray, staff have taken calls from people posing as others to obtain information they don't have a right to. Parents might not understand that they don't have the right to ask for information on their grown children, she adds. "Some people are nosy. There are a lot of family dynamics that can come into play," she says. "If we start asking detailed questions, they will usually just hang up." ■

Registration kiosks made 'intuitive' for patients

The Medical Center of Central Georgia in Macon was an early adopter of registration kiosks, says **Jane Gray**, CPA, FACHE, FHFMA, assistant vice president for the revenue cycle. When they were first implemented in 2007, she says, other hospitals were skeptical they could work.

"Now, their boards are approving this concept," she says.

The kiosks first were placed in the hospital's Heart Services area, then the diagnostic center, says Gray. "Over time, we deployed it in other locations. We put kiosks in the family practice environment, and most recently, in both the main surgery and ambulatory surgery centers," she says.

The kiosks are not completely self-service, because staff members are available to assist patients with navigating the system, says Gray. "We were still able to realize significant cost savings, since staff members can manage multiple kiosks at one time," she says. "However, our platform was the same one we went live with four years ago and was somewhat outdated."

Patients occasionally complained that the system was difficult to use and wasn't intuitive enough, Gray explains. For example, it included a "yes or no" checkbox that didn't allow users to click inside the "yes" box, and it didn't have a "back" button on every screen, she says. "When you are first starting out with kiosks, you might not think about little things that can make a difference to a patient," says Gray.

EXECUTIVE SUMMARY

A growing number of patient access departments are utilizing registration kiosks, but patients might complaint that they are difficult to use. To make kiosks user-friendly:

- Include a "back" button on every screen.
- Have patients complete a survey after use.
- Address identified problems right away.

An updated version recently was rolled out, and it makes the process much simpler for users, says Gray. "People can perform the registration more independently," she says. "Feedback so far has been just wonderful." Patients complete a brief survey after the registration is complete, so that any problem can be addressed right away, Gray says.

Simplicity is goal

Registration kiosks will be added to other areas of the hospital this year, including the urgent care center and ED, says Gray.

"Our methodology was really to address the high-volume peaks-and-valley locations where we could really get some staff savings," she says.

The next step might be enabling patients to register themselves using smart phones, Gray says. "As advanced as health care is in terms of medical technology, we're fairly slow to react to things that have been around in other industries for a long time," she says. "I want to see a registration app. That is where life and technology are going."

Gray says, "To me, it's all about making it simpler for the patient," she says. "In the future, instead of capturing the information on the kiosk, maybe patients will check in on their iPhone as they pull into the parking deck." ■

An ED patient can't pay? Don't leave them hanging

Have staff offer aid with finances

At Catholic Health Initiatives in Lincoln, NE, the patient access department is forming a workgroup to do a better job of helping patients with financial counseling at the time of their emergency department (ED) visit, says **Lauree M. Miller**, director of patient access.

"If it's an emergency situation, it's difficult

to have that conversation with patients," she acknowledges. "They are concerned about their condition. They were not planning to come in, so they didn't have any time to think about how they will pay."

However, Miller says that ED patients are getting more comfortable discussing finances, and staff are getting more comfortable asking them for payment. "We incorporate it into our scripting and hardwire it into the work that we do," she says. "Even asking the question is a shift. Before, it was always just 'we'll just send you a bill.'" The department has seen some recent increases in its ED cash collections, says Miller, but "probably not where we want it to be."

The workgroup was formed due to the growing numbers of self-pay patients in the ED, says Miller. "We are looking at what we can do to help ED patients with financial assistance counseling," she says. "Are we just giving them a form, or do we have a good process in place to close the loop? This is an area we feel we really need to close the gap."

It's not enough to simply hand the patient an application for Medicaid or the hospital's financial assistance program, says Miller. "The paperwork may seem overwhelming and complicated to the patient," she says. "We don't want the bill to go to a collection agency down the pike, when the patient really didn't have the ability to pay in the first place."

Miller says that some ED patients have been "very grateful for our assistance. It's all in our scripting and how we reach out to them. We want to be sure they have an avenue to come back to the facility for assistance."

Offer a service

While scripting can help registrars to discuss finances initially, staff ultimately are most comfortable using their own words, says Miller.

"We did some role playing. This gave staff the chance to practice dealing with some of the more difficult customers," she says.

Staff are reminded to remember that being asked for payment is new for ED patients, says Miller. "People aren't used to paying upfront at a hospital. It's a change," she says.

Likewise, registrars are not accustomed to being financial counselors, says Miller. "That is a mindset change for them, as well," she says. "We are getting staff comfortable by doing role play after role play. Still, some have told us, 'I wasn't hired to call people and ask them for money.'"

Miller says that while registrars are given additional training and support in this role, some have remained resistant. "Staff have to meet us halfway. They have to want to do this," she says. "If it's not something they could ever get comfortable doing, we help them recognize that this isn't the position for them."

Patients are more likely to respond positively to collection attempts if staff present it to them as a service being offered, says Miller. For instance, staff may say to a patient, "We'd like to provide a service to you, to help you understand your coverage and your out-of-pocket responsibilities. Can we put a down payment on your visit today, to reduce your bill when you do get it in the mail?'" she says.

"If you start out that way, patients are much more willing to listen," says Miller. *(See related stories on real-time insurance verification, p. 58, and working with clinical staff, p. 58.)*

SOURCE

For more information on ED collections, contact:
• **Lauree M. Miller**, Director, Patient Access, Catholic Health Initiatives, Lincoln, NE. Phone: (402) 219-5488. Fax: (402) 219-8008. E-mail: laureemiller@catholichealth.net. ■

EXECUTIVE SUMMARY

Financial counseling at the time of a self-pay patient's emergency department visit might improve collections and satisfaction. To help ED patients:
• Do role playing to increase comfort level of staff.
• Present financial counseling to patients as a service being offered.
• Verify coverage in real time.

Tools for ED collections: Verify coverage now

"I can't pay today." "That's ridiculous. I never had to do that before." "Just bill me for it."

These statements are commonly heard by emergency department (ED) registrars, reports **Lauree M. Miller**, director of patient access at Catholic Health Initiatives in Lincoln, NE.

However, Miller says that these responses are becoming less common because patients are

becoming accustomed to being asked for payment. "We sincerely listen to patients. Then, we offer an explanation," she says.

Because it's difficult to estimate ED charges at the time of the patient's visit, only copays are collected, Miller says. The actual charges aren't always known at the time the patient leaves the ED, she says. "If a patient comes in with a fall injury and gets an X-ray and a CT scan, those charges might not be entered by the time the patient leaves," she explains.

Also, the patient's deductible might change by the time he or she receives a bill, Miller adds. "By the time our bill goes out the door, the insurance company may have paid off more bills from their physicians," she says. "It's a snapshot in time, so the patient's deductible could change from day to day."

Registrars now are using an insurance eligibility verification tool, telling them within seconds if the patient's coverage is valid and the amount of the ED copay, reports Miller. "We only have it set up right now for our top 10 payers," she says.

When the hospital system set out to increase its point-of-service cash collection, the inability to verify a patient's eligibility at the time of registration was identified as a major stumbling block, says Miller. "We wanted to put more resources on the front end in capturing that information, rather than getting a denial on the back end," she says. "We know that when the patient leaves us, the chance of us getting that information significantly declines."

If a patients give an expired insurance card, staff member are able to ask them whether they have another card or whether they changed plans recently, she says. "We can at least have a conversation," says Miller. "Staff can say, 'It looks like you are not eligible. This expired on Dec. 31 of 2010. If we run it through, it will come back as a denial.' The patient doesn't want a surprise, either."

It might be that the patient does have coverage but it needs to be updated, she adds. "It may be that the subscriber is the patient and not her spouse," she says.

If the patient says he or she can't pay the entire ED copay, staff will ask the patient to pay something, says Miller. "We take a conservative approach, but people are getting used to us requesting payment," she adds. "It's not as big of a surprise as it might have been six months ago." ■

With ED POS collection, clinical areas are the key

Staff must convey the urgency

If you want to increase point of service collections in the emergency department (ED), communication with clinical staff is the key, says **Lauree M. Miller**, director of patient access at Catholic Health Initiatives in Lincoln, NE.

After the patient is stabilized and seen by a physician, says Miller, the ED tracking board is flagged by clinical staff to let registrars know that Emergency Medical Treatment and Labor Act (EMTALA) requirements have been met.

"The board is color-coded, to let them know when it's OK to go to the patient's room," she says.

Miller says that the physical layout of the ED requires the patient to stop by a checkout desk before leaving. Registrars scan the tracking board, she says, so they don't interfere with patient throughput. "Registrars understand the urgency of getting patients through the process as quickly as possible," she says. "Clinical staff know there's a fine line for when we can have that conversation with the patient."

The key is to be sure that clinical staff comprehend the importance of point-of-service collection, says Miller. "The clinical staff need an appreciation for the registration process, and vice versa," she says. "Everybody has things that they are responsible for getting done and documented, both in the registration world and the clinical world." ■

Patients expect registrars to educate them

Many uninformed about coverage

More often, registrars are finding themselves in the difficult position of educating patients about their insurance coverage, according to **Steph Collins**, manager of patient access at Fairview Northland Health Services in Princeton, MN.

"We are definitely finding it necessary to help patients understand their insurance plans," says Collins. "Some patients are surprised to learn they have a deductible and co-insurance."

Many plans are changing now from a co-pay to a deductible or co-insurance plan, says Collins,

and registrars find themselves explaining what that change means to the patient. For example, she says, a patient might present to the emergency department and find out after speaking with registrars that they have a large deductible, when they thought they had a co-pay only.

"Some patients just do not understand what a deductible is or what it means to them," says Collins.

As a service to patients with scheduled services, registrars are informing them of their potential out-of-pocket expenses, says Collins. "Some people are shocked, because they didn't realize they had a deductible or co-insurance," she says. "A few patients choose to cancel or seek alternative services with their provider that are at a lower cost for them at the moment."

Calm under pressure

"The best thing to do with patients who are upset or concerned about their coverage or out-of-pocket expenses is to explain as best we can what their coverage means to them," says Collins.

At Virginia Mason Medical Center in Seattle, staff member answer questions for patients about their insurance, to a certain degree, says Angela Cabarteja, supervisor in patient financial services. "You do have to be careful not to go too in-depth, because each plan can vary so much," she says.

Staff often explain how much the deductible, co-insurance, and out-of-pocket maximums are, and how much the insurance shows has been met so far, says Cabarteja. "The patient usually just wants to know how much they will be responsible to pay out of their own pocket," she adds.

When a patient becomes upset or frustrated, says Cabarteja, staff work hard to remain calm and understanding. "Insurance can be very confusing, even when you are in this line of work and deal with it every day," she adds.

Staff members might be able to think of another way to explain a particularly confusing point or ask if a caller would like to come in to review the information in person, she says. If staff aren't able to answer specific details about a person's coverage, they'll offer to have someone from the insurance company call to discuss it, says Cabarteja. "Unfortunately, there are times when you do have to refer them back to their insurance company for more specific details," says Cabarteja. *(See related story about giving patients financial options, p. 60.)*

EXECUTIVE SUMMARY

Patient access staff are increasingly being asked to explain patients' insurance coverage, including deductibles and co-insurances. Use these strategies:
- Explain what patients are responsible for.
- Ask if a caller wants to review the information in person.
- Offer to have the insurance company contact the patient.

SOURCES

For more information on educating patients about their insurance coverage, contact:

- **Angela Cabarteja**, Patient Financial Services, Virginia Mason Medical Center, Seattle. E-mail: Angela.Cabarteja@vmmc.org.
- **Steph Collins**, Manager of Patient Access, Fairview Northland Health Services, Princeton, MN. Phone: (763) 389-6263. Fax: (763) 389-6446. E-mail: scollin1@fairview.org.
- **Todd Shoaf**, Director of Patient Accounting, Moses Cone Health System, Greensboro, NC. Phone: (336) 832-8014. Fax: (336) 832-8583. E-mail: Todd.Shoaf@mosescone.com.

Large out-of-pocket? Offer patients options

Come up with a solution

At Fairview Northland Health Services in Princeton, MN, when patients learn they will have a large out-of-pocket responsibility, patient access staff work with them to explain their payment options, says **Steph Collins**, manager of patient access.

"Within the last six months, we started using a new tool that helps us set up monthly payment plans using patient's credit or debit cards," she reports.

Patients are able to have a prearranged amount paid to their medical account each month through their credit card, or their checking or savings

COMING IN FUTURE MONTHS

- Dramatically increase your copay collection
- Put a stop to abuse of financial assistance programs
- Invest in technology to tell patients what they'll owe
- Strategies to obtain all authorization requirements

account, explains Collins. "This is new for our patients," she says. "Many have commented on how much they appreciate it. They no longer have to remember to send in their monthly payment for their medical bills."

Staff also screen patients to determine if they are eligible for the hospital's charity care program, says Collins. Staff refer patients to their employer or insurance agent if they think the information is incorrect, she adds. "Most importantly, we let the patient know we're here to help," says Collins. "Most of the time, we can work with the patient to come up with a solution that meets their needs and expectations."

Angela Cabarteja, supervisor in patient financial services at Virginia Mason Medical Center in Seattle, says that her patient access staff have "a lot of financial options" to offer. For instance, staff can provide a screening for the state Department of Social and Health Services and offer assistance completing an application, she says. Staff can offer patients varying levels of charity based on the federal poverty guidelines and the patient's income, or payment arrangements can be made, says Cabarteja. "We try to identify these concerns prior to the patient having a service, so we can eliminate the guesswork," she says.

If a patient qualifies for charity upfront, she explains, the patient knows he or she won't have a balance after insurance. "This puts the patient at ease, so they can focus on their care and recuperation," she says.

Screen inpatients

At Moses Cone Health System in Greensboro, NC, financial counselors try to interview every self-pay inpatient while they are still in-house, to screen them for possible Medicaid eligibility as well as state and local programs, says **Todd Shoaf**, director of patient accounting.

"We average about $1.3 million in conversions weekly," he reports. "We routinely convert many accounts weekly from self pay to some type of sponsorship."

Staff members ask patients questions based on what the state Department of Social Services (DSS) will be looking for and review their medical records for possible long-term disability, says Shoaf. "If we feel Medicaid is an option, we schedule an appointment for the patient with a local DSS representative located onsite in the hospital to fill out a Medicaid application," he says.

Patients complete the application while they are still in the hospital, says Shoaf, and the financial counseling staff follows the case with DSS to find out where they are in the approval process, until a decision has been made. "Additional medical information or information from the patient may be needed," he says.

If the patient ultimately is approved, this approval benefits the hospital and the patient, says Shoaf. "The patient doesn't have to worry about how they're going to pay their bill, and the hospital receives some reimbursement for the services provided," he says. ■

EDITORIAL ADVISORY BOARD

Pam Carlisle, CHAM
Corporate Director PAS, Revenue Cycle Administration
Columbus, OH

Raina Harrell, CHAM
Director, Patient Access and Business Operations
University of Pennsylvania Medical Center-Presbyterian
Philadelphia

Holly Hiryak, RN, CHAM
Director, Hospital Admissions
University Hospital of Arkansas
Little Rock

Beth Keith
Manager
Healthcare Provider, Consulting
Affiliated Computer Services Inc.
Dearborn, MI

Peter A. Kraus, CHAM
Business Analyst
Patient Accounts Services
Emory University Hospital
Atlanta

Keith Weatherman, CAM, MHA
Associate Director
Patient Financial Services
Wake Forest University Baptist Medical Center
Winston-Salem, NC

John Woerly, RHIA, CHAM
Senior Manager
Accenture
Indianapolis

To reproduce any part of this newsletter for promotional purposes, please contact: *Stephen Vance*
Phone: (800) 688-2421, ext. 5511
Fax: (800) 284-3291
Email: stephen.vance@ahcmedia.com

To obtain information and pricing on group discounts, multiple copies, site-licenses, or electronic distribution please contact: *Tria Kreutzer*
Phone: (800) 688-2421, ext. 5482
Fax: (800) 284-3291
Email: tria.kreutzer@ahcmedia.com
Address: AHC Media
3525 Piedmont Road, Bldg. 6, Ste. 400
Atlanta, GA 30305 USA

To reproduce any part of AHC newsletters for educational purposes, please contact:
The Copyright Clearance Center for permission
Email: info@copyright.com
Website: www.copyright.com
Phone: (978) 750-8400
Fax: (978) 646-8600

HIPAA Regulatory Alert
Supplement to *Healthcare Risk Management* and *Hospital Access Management*

Million-dollar-plus fines signify tougher enforcement of HIPAA

HITECH rules pave way for much higher penalties

Fines of $4.3 million for Maryland-based Cignet Health and $1 million for Massachusetts General Hospital in Boston should give hospital staff reason to take notice of the stricter enforcement and higher fines included in the Health Information Technology for Economic and Clinical Health (HITECH) Act.

"Although many compliance officers see these headlines and are thankful it wasn't their organization, the real message in all of the news stories from OCR [Health and Human Services' Office of Civil Rights] was the OCR representative's repetition of the statement that OCR is serious about enforcing HIPAA regulations," says **Helen Oscislawski**, Esq., principal with Attorneys at Oscislawski, Princeton, NJ. "Also, each case that is prosecuted gives compliance officers a snapshot of what led to the violation and what OCR expects the organization to do to bring their organization into compliance."

Because the resolution agreements between OCR and institutions found to be in violation of HIPAA privacy or security rules are published on the Health and Human Services' web site, compliance officers can see what actions OCR expects the organization to take, says Oscislawski. *(See resources, p. 2, for web site information.)* "With each resolution agreement posted, it becomes more difficult for a compliance officer to say he or she didn't know OCR expected policies or compliance programs to contain certain elements," she explains. "These resolution agreements should be reviewed by all compliance officers when they are posted."

The agreements can serve as a checklist in the evaluation of an organization's own compliance program, she adds. For example, in the Massachusetts General case, an employee took paper copies of medical records home to finish some work, says Oscislawski. "The next day, when going to work, she forgot to pick up the bag containing the records and left them on the subway," she explains. The resolution agreement for Massachusetts General includes the $1 million fine along with a requirement to revise policies to address removal of protected health information (PHI) from the hospital premises, Oscislawski says. Although paper documents were involved in this case, the agreement also provides for Massachusetts General to address encryption of PHI on laptops, flash drives, and other electronic media, she points out.

"HIPAA does not mandate the use of encryption for all PHI, but in this and other resolution agreements, encryption is often required," she says. "Al-

EXECUTIVE SUMMARY

Everyone knew that the Health Information Technology for Economic and Clinical Health (HITECH) Act increased the penalties for non-compliance with HIPAA privacy and security rules. However, a $4.3 million fine for Maryland-based Cignet Health and $1 million for Massachusetts General Hospital in Boston reinforced that the Office of Civil Rights (OCR) is serious about enforcement.

- Review resolution agreements and corrective action plans posted on OCR's web site (www.hhs.gov/ocr/privacy) to determine best practices.
- Develop policies that limit removal of protected health information from hospital premises.
- Use tools such as New York University Langone Medical Center's "badge buddy" to ensure employees know when and who to call with questions or concerns about compliance.

though encryption is not required, it is obviously viewed as a best practice."

When it comes to removal of PHI from the premises, it is difficult to say an employee should never remove information, due to the nature of some people's work, says **Dave Sina**, JD, vice president of compliance for Healthcare Compliance Consulting in St. Paul, MN. "The best policy related to removal of PHI from the premises is one that allows it for specific reasons and only with the approval of an upper level manager," Sina suggests. "Approval should be given after the reason is identified, the identity of the person is clear, and the steps to protect the information is clarified."

The Cignet Health case is not a case of removal or loss of PHI, but instead it focuses on the organization's refusal to provide 41 patients with copies of their medical records within the 30 to 60 days of the request, says Oscislawski. The $4.3 million civil monetary penalty imposed on Cignet Health could have been avoided by simply responding to the reasonable requests of patients for their own medical records, according to the case laid out by the Department of Health and Human Services (HHS), she points out. "It is not yet clear why Cignet denied patients access to their records but there is no reason to withhold a patient's records," she adds.

Even though Cignet failed to give patients access to records, the size of the fine could have been reduced if the organization had responded to letters from HHS and cooperated with the investigation, says Oscislawski. Eventually, Cignet produced the records requested by HHS, but they included them in 59 boxes that included 4,500 patient records, she says.

"It's ironic that when they provided the records requested, they also disclosed that many other records for which there was no reason to disclose," Oscislawski adds.

HITECH allows extra penalties

The lesson to learn from the Cignet fine is to work with OCR, Oscislawski says.

"The initial fine for denying patients access to their records in a timely manner was $1.3 million, but an additional $3 million was added for failure to cooperate with OCR and to provide the records within the timeframe set during the investigation," she says.

The punitive fines are a key feature of HITECH, Sina says. "An organization can be fined up to $50,000 per day per violation," he explains. In Cignet's case, the organization showed "willful neglect" and failed to cooperate in the investigation from March 17, 2009, to April 7, 2010, he adds.

"Prior to HITECH there was no opportunity for OCR to assess [triple] damages, which has been done in some cases, or to assess additional penalties based on number of violations," Sina explains. Although smaller healthcare organizations might have taken a chance in the past and chosen not to implement HIPAA compliance programs due to cost, the potential for additional fines makes compliance more important than ever, he adds.

In addition to enhancement of policies, a key component of most resolution agreements is the provision and verification of employee education. Not only do employees need to understand the hospital's policies about protection of PHI, but also they need to know how to report potential breaches, says Oscislawski. *(See "Badge buddy" on p. 3.)*

"I don't have a crystal ball," admits Oscislawski. "I do, however, see stricter enforcement and larger fines for HIPAA and HITECH violations to continue."

SOURCES/RESOURCES

For more information about tips to improve compliance, contact:

• **Nancy Dean**, JD, MPA, CHC, CHRC, Vice President of Audit and Compliance Privacy Officer, NYU Langone Medical Center, 550 First Ave., New York, NY 10016. Telephone: (212) 404-4078. E-mail: Nancy.Dean@nyumc.org .

• **Helen Oscislawski**, Esq., Principal, Attorneys at Oscislawski, 22 Caroline Drive, Princeton, NJ 08540. Telephone: (609) 385-0833. Fax: (609) 385-0822. E-mail: Helen@oscislaw.com.

• **Dave Sina**, JD, Vice President of Compliance, Healthcare Compliance Consulting, 5755 Heather Ridge Drive, St. Paul, MN 55126. Telephone: (651) 484-4303. Fax: (651) 484-6213. E-mail: davesina@q.com.

• To see copies of **resolution agreements and press releases regarding HIPAA cases**, go to www.hhs.gov/ocr/privacy and select "news archive" on the left navigational bar. Scroll through the press releases to find copies of descriptions of fines and investigations, resolution agreements, and corrective action plans with Massachusetts General (2/24/2011), Cignet Health (2/22/11) as well as other organizations.

• To see a copy of the **New York University Langone Medical Center "badge buddy"** and read more about the compliance program, go to http://compliance.med.nyu.edu. Select "Help line" from the top navigational bar. ■

'Badge buddy' provides HIPAA info

All staff have access to compliance hotline

Even before headlines highlighted large fines for HIPAA violations, the compliance department at New York University (NYU) Langone Medical Center in New York City decided to be proactive to meet the enhanced requirements of the Health Information Technology for Economic and Clinical Health (HITECH) Act.

"With the stringent timeframes for the reporting of potential breaches set in HITECH, we want to make sure employees understand the importance of contacting our office immediately," explains **Nancy Dean**, JD, MPA, CHC, CHRC, vice president of audit & compliance privacy officer for NYU Langone. In addition to training sessions for all employees, the staff developed a "badge buddy" that ensures all employees can easily reach the compliance office when needed. (See resources, p. xxx.)

"The badge buddy is a small, plastic card that attaches to an employee's name badge," says Dean.

The card includes telephone numbers for a compliance helpline to answer compliance questions as well as a separate helpline for protected health information and HIPAA privacy concerns. "Everyone always has their name badge, and the badge buddy ensures that they always have our information as well," Dean says.

The card also includes a short list of reasons to call the protected health information (PHI) helpline such as having a laptop stolen, finding unsecured patient information, or sending a fax with patient information to the wrong number, she adds.

The badge buddies have led to about 70 calls from employees since the program was implemented in early 2010, says Dean. Samples of calls include questions about whom to call to shred documents and whether receipt of a fax from outside the hospital that was meant for someone else was a HIPAA violation, she says. "In the case of receiving a fax in error, it provided a good teaching moment as we explained to the employee that since we did not generate the fax, we were not liable," she says. "In fact, the calls we get on the helplines help us tailor our ongoing education to address the most frequently misunderstood issues," she adds.

Although the key to consistent compliance with HIPAA privacy and security regulations is ongoing education, it is essential to adapt educational messages and reflect what is important, Dean says. "We need to keep education meaningful and fresh," she says. "Otherwise, people stop listening because they are not hearing anything new." ■

Beware of breach sources: Laptops and flash drives

Passwords, encryption, and VPNs cut risks

Fifty percent of data breaches are related to theft of portable or easily moved devices such as laptops, flash drives, and desktop computers, according to the most recent report from the Health Information Trust Alliance, a national consortium of healthcare professionals that focuses on healthcare data security.[1]

Employees at Henry Ford Health System (HFHS) in Detroit know that these statistics are true after experiencing the theft of a laptop from an office and a flash drive dropped in a parking lot in a three-month span of time.

"The laptop was stolen when an employee left his office door unlocked so his secretary could get something from it while he was gone," explains **Meredith Phillips**, MHSA, CHC, CHPC, chief privacy officer in the office of corporate compliance for HFHS. Due to a delay in the discovery that the laptop was missing and a further delay in notifying Phillips' office, 54 days passed before the hospital notified patients about the potential breach, she says. "This was within the 60-day time limit set by HITECH, but it took longer than we want it to take," she adds.

The publicity of the potential loss of data and additional training increased all HFHS employees' awareness. Less than three months later, a resident discovered that a flash drive had fallen off his key chain at some point while he was at dinner away from the hospital. A report was made to Phillips' office. "Because he reported it immediately and because he had stored a copy of the information he downloaded to the drive on the hospital's server, we were able to quickly identify which patients were affected," she says. Patient notification of the potential breach was made in 18 days for this incident, she adds.

The portability of laptops and flash drives increases convenience for employees who want to work at home, but they are easily stolen or lost, points out **Marion Jenkins**, PhD, FHIMSS, founder and chief executive officer of Englewood, CO-based QSE Technologies, which provides IT consulting for healthcare organizations. "I include

desktop computers as portable devices in my own analysis because they are located at the edge of the network and on users' desks, which are often accessible by non-users," he explains.

Passwords not enough

Passwords can help protect the information, but many healthcare personnel don't use passwords appropriately, Jenkins says.

"There may be a password for the nursing station computer, but it is often a shared password for all of the nurses to make it simpler to access information," he says. "Shared usernames and passwords can be easily defeated by someone who wants to access the information."

The best protection is not to allow storage or downloads of any protected health information (PHI) to a laptop, flash drive, or desktop computer, says Jenkins. "Files and data should be stored on a server and accessed over the office local area network, or if the user is remote, over a secure VPN [virtual private network] connection," he says.

If employees do store information on laptops or flash drives, be sure they are encrypted, warns Jenkins. "Even if the laptop is stolen out of the employee's car, the thief must have the encryption key to access the information," he adds.

Because HFHS is a teaching hospital and many employees are involved in research, it is inevitable that people will need to download information onto a portable device, Phillips points out. "We've chosen to encrypt all portable devices used by HFHS employees," she says.

The ambitious program to identify and encrypt or replace portable devices used by the 24,000 health system employees started in late March 2011 with a 10-day event designed to identify all laptops, external hard drives, and flash drives. Stations located throughout the health system were manned by information technology staff from 6 a.m. to 6 p.m., she says. "We replace all unencrypted flash drives with encrypted drives and transfer the information for the employee, and we inventory all laptops and external hard drives and encrypt them as well," she says.

If an employee has a device that cannot be encrypted, HFHS will replace it with a laptop or hard drive that is encrypted, she adds. Phase II of the program, which will begin later in 2011, will address other devices such as smart phones and digital voice recorders, she says.

In addition to encrypting existing devices, Phillips department worked with information technology and purchasing to ensure that the only devices that will be issued to employees from this point comply with policies set by her department.

Enhanced educational efforts and a zero tolerance policy will protect HFHS from potential breaches, says Phillips. "Once we have successfully encrypted all devices, employees are expected to use them, not their personal, unencrypted devices," she says. "Employees who make a decision to use an unencrypted device to store PHI will be subject to termination."

REFERENCE

1. Hourihan C. An Analysis of Breaches Affecting 500 or More Individuals in Healthcare. Health Information Trust Alliance, Frisco, TX. August 2010.

SOURCES

For more information about the risks of portable media, contact:

• **Marion K. Jenkins**, PhD, FHIMSS, Founder and Chief Executive Officer, QSE Technologies, 359 Inverness Drive S., Suite K, Englewood, CO 80112. Telephone: (303) 283-8400. Fax: (303) 283-8401. E-mail: marion.jenkins@qsetech.com.

• **Meredith R. Phillips**, MHSA, CHC, CHPC, Chief Privacy Officer, Office of Corporate Compliance, Henry Ford Health System, 2799 W. Grand Blvd., Detroit, MI 48202. Telephone: (313) 874-5168. Fax: (313) 874-5608. E-mail: mphilli2@hfhs.org. ■

Meaningful use FAQs added by Medicare

Eleven new questions and updated answers to other questions about the Meaningful Use Incentive Program can be found on the Centers for Medicare and Medicaid Services (CMS) web site.

The new FAQs clarify the term "reasonable cost" for critical access hospitals and whether eligible professionals and eligible hospitals must demonstrate meaningful use in the exact way that electronic health records technology was tested and certified.

To access the FAQs, go to www.cms.gov. Choose "Regulations and Guidance," then under the "Legislation" heading, select "EHR Incentive Programs." Scroll down to the bottom of the page. Under "Related links inside CMS," select "Frequently Asked Questions." *(For more information about meaningful use incentives, see* HIPAA Regulatory Alert, *February 2011, p. 1.)* ■

Hospital Access Management

Admitting * Reimbursement * Regulations * Patient Financial Services * Communications
Guest Relations * Billing & Collections * Bed Control * Discharge Planning

2011 Reader Survey

In an effort to learn more about the professionals who read *Hospital Access Management*, we are conducting this reader survey. The results will be used to enhance the content and format of the publication.

Please fill in the appropriate answers or write your answers to the open-ended questions. Return the questionnaire and answer sheet in the enclosed postage-paid envelope by **July 1, 2011.**

1. Are the articles in *Hospital Access Management* written about issues of importance and concern to you?

O A. always O B. most of the time O C. some of the time O D. rarely O E. never

Here is a list of hospital access issues. For each item, please circle your answers accordingly:

	A. should cover it more	B. about right	C. should cover it less	D. don't know/no answer
2. Admissions/registration	O A	O B	O C	O D
3. Billing/reimbursement	O A	O B	O C	O D
4. EMTALA	O A	O B	O C	O D
5. Confidentiality/HIPAA	O A	O B	O C	O D
6. Customer service	O A	O B	O C	O D
7. Discharge planning	O A	O B	O C	O D
8. Scheduling	O A	O B	O C	O D
9. Staffing/recruitment needs	O A	O B	O C	O D
10. Technology	O A	O B	O C	O D
11. Training/education	O A	O B	O C	O D

12. How would you rate your overall satisfaction with your job?

O A. very satisfied O B. somewhat satisfied O C. somewhat dissatisfied O D. very dissatisfied

13. How would you describe your satisfaction with your subscription to *Hospital Access Management*?

O A. very satisfied O B. somewhat satisfied O C. somewhat dissatisfied O D. very dissatisfied

For each item below, please fill in your answers accordingly:

	A. excellent	B. good	C. fair	D. poor
14. Quality of newsletter	O A	O B	O C	O D
15. Article selections	O A	O B	O C	O D
16. Timeliness	O A	O B	O C	O D
17. Quality of supplements	O A	O B	O C	O D
18. Length of newsletter	O A	O B	O C	O D
19. Overall value	O A	O B	O C	O D
20. Customer service	O A	O B	O C	O D

21. On average, how much time do you spend reading each issue of *Hospital Access Management*?

O A. less than 10 minutes O B. 10-20 minutes O C. 21-30 minutes O D. 31-60 minutes O E. more than an hour

22. On average, how many people read your copy of *Hospital Access Management*?

O A. 1-3 O B. 4-6 O C. 7-9 O D. 10-15 O E. 16 or more

23. On average, how many articles do you find useful in *Hospital Access Management* each month?

O A. none O B. 1-2 O C. 3-4 O D. 5-6 O E. 7 or more

24. Do you plan to renew your subscription to *HAM*? O yes O no
If no, why not? _____

25. To what other publications or information sources about access management do you subscribe?

26. Which publication or information source do you find most useful and what do you like most about the publication?

27. What is your title? (please circle the title that most closely reflects your position and responsibilities):

O A. Director of access management O B. Manager of patient accounts O C. Supervisor
O D. Patient account representative O E. Other (please specify) _____

28. What is the highest degree that you hold?

O A. High school O B. Associate's degree O C. Bachelor's degree
O D. Master's degree O E. Other (please specify) _____

29. Please list the top three challenges you face in your job today. _____

30. What do you like most about *HAM*? _____

31. What do you like least about *HAM*? _____

32. What issues would you like to see addressed in *HAM*? _____

Contact information _____