Hospital Access Management™

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

THOMSON
AMERICAN HEALTH CONSULTANTS

IN THIS ISSUE

JULY 2003
VOL. 22, NO. 7 • (pages 73-84)

Want to get a handle on denials? Use these components for best practice

A central clearinghouse for all rejections is a must

In these times of dwindling health care reimbursement, there's no phrase more significant to access managers — and their bosses — than "denial management."

There are several key components that must be in place if a hospital is to achieve best practice in denial management, says **Joe Denney**, CHAM, director of revenue management at The Ohio State University Medical Center in Columbus.

"The goal, of course, is not to receive any [denials] if possible," he notes. To move in that direction, he suggests the following.

In his organization, Denney first notes, a distinction is made between rejections and denials, which is key to understanding the process.

"In our lingo, whenever a claim goes out the door and something comes back from the payer saying it is seeking more information or saying, for example, 'I will deny the last day of this inpatient stay,' we call that a rejection."

Hospital staff work all rejections, he explains, with the aim of turning them around if there is a reason to do so. "A lot of times, a rejection has to do with documentation, as when it says that [access personnel] didn't pre-cert or preauthorize."

That particular type is sent to the registration quality assurance manager, who looks in the system and may say, 'We did do the authorization and here's the authorization number.'" In that case, he adds, "we would write a quick appeal letter and get the money."

What his hospital considers denials, Denney explains, is if a rejection already has been appealed, and the payer has come back and said, "No way we're going to pay." At that point, he says, "we write it off to bad debt. So there's a real distinction between rejection and denial."

That distinction made, he says, the central component of successful denial management is one area in the hospital where all rejections and denials are received.

"Until we established that here [rejections and denials from payers],

went everywhere — to the director of utilization review (UR), the business office, even hospital administration or the chief operating officer. We found it extremely important to have one designated area, and say, 'This is the address.'"

To clarify that, Denney suggests making sure the language is in the managed care contracts. With Medicare, it's not an issue, he adds, because those communications are sent electronically.

"We also did some internal communication, saying, 'If you get these [rejections or denials], forward to this person in the central business office and that person will get in touch with the insurer.'"

Hospital Access Management™ (ISSN 1079-0365) is published monthly by Thomson American Health Consultants, 3525 Piedmont Road, Building Six, Suite 400, Atlanta, GA 30305. Telephone: (404) 262-7436. Periodicals postage paid at Atlanta, GA 30304. POSTMASTER: Send address changes to **Hospital Access Management**™, P.O. Box 740059, Atlanta, GA 30374.

Subscriber Information

Customer Service: (800) 688-2421 or fax (800) 284-3291, (customerservice@ahcpub.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), $465. Outside U.S., add $30 per year, total prepaid in U.S. funds. Two to nine additional copies, $372 per year; 10 to 20 additional copies, $279 per year; for more than 20 copies, call customer service for special handling. Missing issues will be fulfilled by customer service free of charge when contacted within 1 month of the missing issue date. **Back issues**, when available, are $78 each. (GST registration number R128870672.)

Editorial Questions

Call **Christopher Delporte** at (404) 262-5545.

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: **Lila Margaret Moore**, (520) 299-8730.
Vice President/Group Publisher: **Brenda Mooney**, (404) 262-5403, (brenda.mooney@ahcpub.com).
Editorial Group Head: **Coles McKagen**, (404) 262-5420, (coles.mckagen@ahcpub.com).
Managing Editor: **Christopher Delporte**, (404) 262-5545, (christopher.delporte@ahcpub.com).
Production Editor: **Nancy McCreary**.

This piece of the process is crucial, Denney points out. "Every [payer] has a deadline. Some say, 'If you don't appeal within 30 days, we're not going to pay no matter what.' If a rejection went to the director of UR, for example, and that department sat on it for a while, you could be past that line."

The next step, he says, is to have a very good grasp of what a rejection is about, so it can be placed on a work list and sent to the appropriate area to be investigated and appealed.

At the focal point of the rejection / denial activity at OSU Medical Center, Denney notes, is the organization's central business office, where **Mark Tennant**, the rejection / denial manager, oversees the process.

In November 2001, Tennant explains, he was given the mission of developing a rejection process using the health system's existing staff and computer technology.

"The flow was to have the business office receive all rejections — whether correspondence, follow-up, or explanation of benefits," he says. These rejections, Tennant adds, would go to employees known as rejection reps, who would review the information and put them in various categories, or "electronic buckets," depending on the reason for the rejection. **(See illustration, p. 75.)**

A service code assigned to each rejection sends it to one of the following buckets:

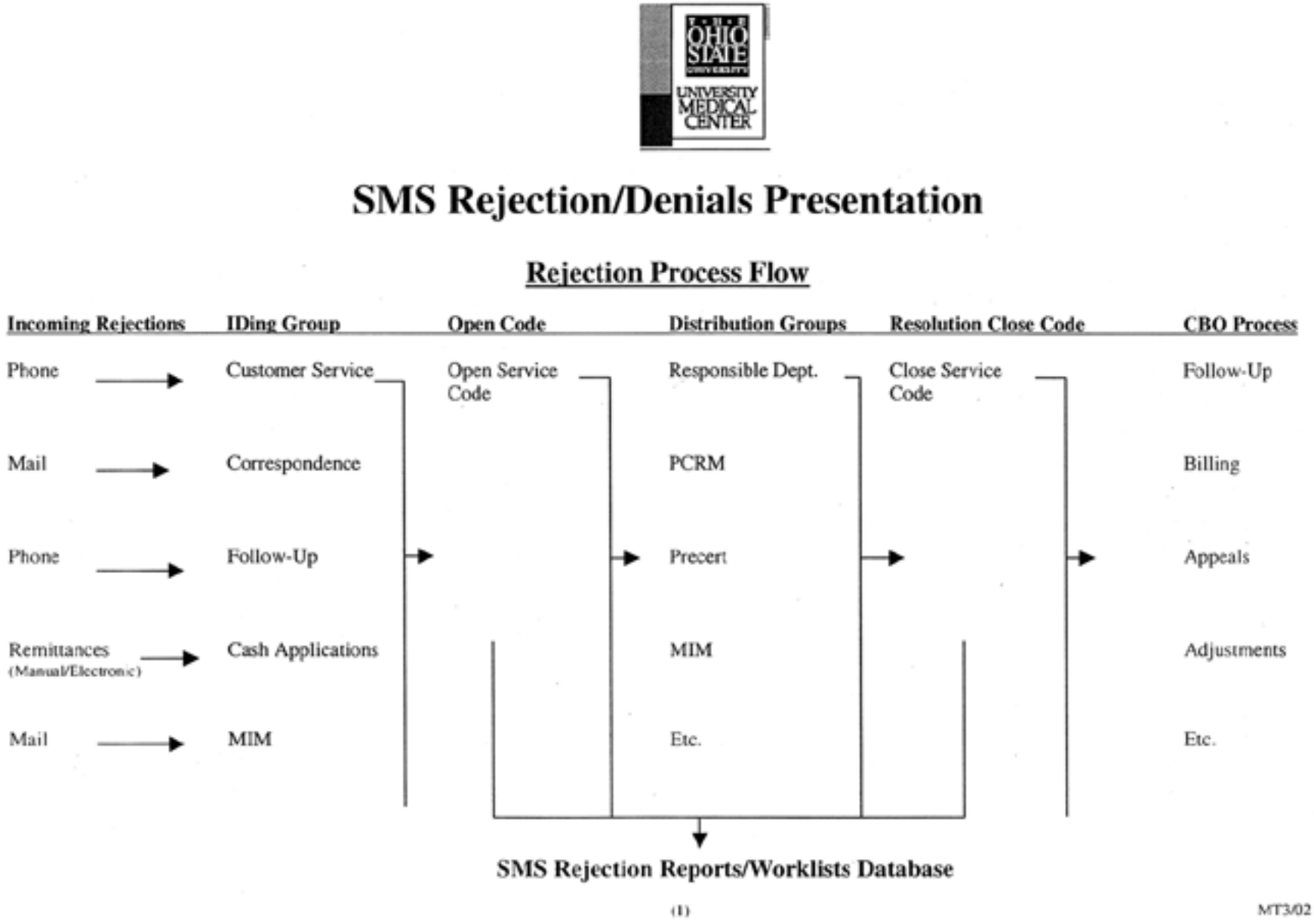
- pre-cert / authorization;
- medical necessity;
- medical documentation;
- peer review organization (PRO) denials;
- Medicaid sterilization.

The latter, Tennant explains, has to do with a consent form that Medicaid requires in order to process claims with a service requiring a "sterilization procedure," such as an abortion or a hysterectomy.

There are more than 50 "open" service codes — defined by the payer's reason for the rejection — within the five categories, he adds, so, for example, there are several reasons why a rejection might go into the pre-cert / authorization bucket. "If authorization date was the problem, the [rep] would apply that [specific] service code."

One individual is assigned as the gatekeeper for each bucket, Tennant says, and that person receives a daily revenue management work list listing all the rejections it contains. While the gatekeepers may hand off the task to other

(Continued on page 76)



Source: The Ohio State University Medical Center, Columbus.

employees, they ultimately are responsible for resolving those rejections.

"Their names are assigned to that work list, which is important for accountability," he notes. "The gatekeeper has 10 days to resolve the account. At that time, they put a 'close code' on it, which shows what the resolution was."

The resolution might be "authorization obtained," "no authorization obtained," "additional information sent," and so forth, Tennant says. "Once [the rejection] is closed, that account goes back into our regular business operation, and the code triggers the next action."

What's unique about the process, he says, is that everything that happens within the service code — a function of the hospital's patient accounting system — is a permanent stamp. "The 'open' and 'close' codes are tracked to the ultimate payment or adjustment to the account, why we opened it and why we closed it."

'Data warehouse' produces reports

As part of the denial management process, the hospital's information services department has developed an information warehouse for the rejection data, Tennant says. In place since September 2002, this data warehouse "is like a [subset] of the process," he adds. "The information is identified and dropped into the warehouse, which produces reports that show a breakout of the buckets."

Those reports show which payers the rejections are coming from and what the problems are, Tennant says. "We can look at the whole process, to see if it's the payer having the issue or a practice we need to change."

Administrators, directors, and managers throughout the hospital system receive biweekly summary reports on the five buckets, including the number of rejections and the related dollar amount.

It's been extremely important to the success of the denial management initiative that "almost all the departments in the hospital" are involved, Tennant says. When he made the initial presentation on the process, he adds, "the right people were in the room to say, 'I can do this; I can help.' That's the plus of doing that."

In addition to putting language into the contract regarding where rejection correspondence should be sent, the managed care department comes into play in communicating with payers at the other end of the process, Tennant points out.

When managed care personnel meet periodically with payers — for some it's quarterly, for others every two months or once a month — they discuss and review denial management reports, he says.

"[The hospital representative] says something like, 'We've boiled it down to what we think the real issue is,'" Tennant says. "If it's a payer problem, [the hospital's position is], 'This is what we're seeing. Tell us why you're rejecting these claims.'"

The managed care department, as well as "everybody under the revenue cycle," has direct access to the denial information, he notes.

The next step is to designate one individual on the payer's side and one individual from the hospital who correspond directly regarding rejections, Tennant adds. The hospital already has this relationship with two of its biggest payers, he says, and the goal is to increase that to five.

(Editor's note: Joe Denney may be reached at Denney-1@medctr.osu.edu. Mark Tennant may be reached at Tennant-1@medctr.osu.edu.) ■

Training, proper plan ID cut denials by $20 million

'Most employees want to do a good job'

Looking at opportunities for improvement after becoming director of patient access at Children's Health Care of Atlanta about two years ago, it was natural that **Millie Brown** would turn her attention to the quality of registration data.

And given the education-focused culture of her organization, adds Brown, a former manager in the billing department, it was natural that staff education would be an important part of her quality improvement initiative.

That initiative, which took place between January and December 2002, turned the spotlight on ensuring proper identification of patients' insurance plans and has resulted in more than 75% of claims being paid the first time out, she says. "The industry standard is 52%, so we're well above that." The positive financial impact on the health system has been approximately $20 million less in annual denials, Brown adds.

Training started with the assumption that

"most employees want to do a good job, and the reason for the errors is they think they're doing it correctly already," she notes. "Using that mindset, we created an insurance card test. We took a sample of the different cards submitted [to registrars], gave a plan code listing, and did a matched quiz."

The idea, Brown adds, was to give employees the opportunity to see that there was room for improvement. "We achieved some motivated learners."

The initiative was aimed not only at the 140 access employees who are Brown's direct reports, but also the access staff at the health system's many satellite clinics, for whom her department oversees training and quality control.

Easier said than done

Identifying the correct plan — with insurance cards covered in different logos and the plan name not always the most prominent — is easier said than done, Brown notes. To show how confusing the process can be, she says, the departmental trainer administered the quiz not only to patient access staff, but also to patient accounting employees and system leaders (vice presidents).

"Often [those outside access] say, 'Just enter the name on the card,' implying that the process really isn't that hard, Brown explains. "When you think about patient accounting and billing, their job is usually set up so they're working with one type of card. It's not like in access."

The quiz gave the outside staff a better understanding of what it's like to be on the front line and how difficult it is to identify the correct plan, she notes.

In keeping with Children's philosophy of "making sure the message always is consistent," Brown says, one person does all patient access training.

To address the insurance card issue, she adds, **Rose Cape**, manager of quality and training, designed "tip sheets" around the appropriate way to handle the various third-party payers. Cape targeted the handful of payers that make up the majority of the organization's business, Brown says, with the idea that would provide the "biggest bang for the buck."

"If three or four payers represent 70% of your business, is it the best use [of resources] to focus on 10 smaller plans?" she points out. "What if you got 70% of your business 100% correct?"

After receiving "some intense training" on the major payers, Brown says, staff were given the tip sheets, which also are available on the health system's education web site. "If any access employee is having problems with one of the top plans, the supervisor can go to the site and print the tip sheet."

As the quality process continues, she notes, the collection of tip sheets will be expanded to include other payers.

The operative phrase for the tip sheets and for all aspects of training has been "Keep it simple," Cape emphasizes. "Use words that are applicable to [staff], that they're familiar with, to get their buy-in. Give examples of when what they've done in the past hasn't worked, and say, 'When you do this, you'll get this result.'"

Regarding the insurance plan issue, Cape adds, she explains to employees that the hospital doesn't get the correct payment when the wrong plan is chosen because it has different contracts with different payers. "Instead of looking [at an insurance card] in this way," she tells them, "look at it knowing the plans we have contracts with."

The format is the same for any type of constructive criticism of staff, Brown notes. "When you do [insert action], what happens is the wrong outcome. A better choice would be [insert correct action], and the positive result would be [the desired outcome]."

Repetition is another important part of the training equation, Cape adds.

Quality check follows training

Once employees were trained on the top payers and the tip sheets, Brown says, she did a quality check on the information. "Today, for example, we gave a huge training [effort] on Blue Cross Blue Shield," she adds. "Then we went back and checked and watched to see if [employees] are [processing those accounts] the right way. I took a sample of accounts — a very large sample — to see who was doing it correctly."

Those still making errors received additional training, Brown says. In some cases, she notes, tip sheets are adjusted after quality checks.

Any big changes in the process are covered at quarterly training sessions, Brown adds, and "in between those is when we're checking quality. If we see a particular problem with a lot of people, [Cape] will send an alert bulletin, with a tip sheet attached, saying, 'Everyone be careful with this.'"

Supervisors are asked to make sure that all employees have read the bulletin and the

accompanying information, she says. "Each supervisor is accountable for the quality scores of the staff and each manager is responsible for the quality scores of the team."

If the supervisor believes it's necessary, the trainer will work one-on-one with an employee who continues to have problems, Brown says. "The tip sheets are so clear, so concise, that [one-on-one time] is not usually needed."

Brainstorming sessions improve quality

Access managers throughout the health system meet with Brown once a month to brainstorm ways to continually improve quality, she adds.

In addition to focusing on proper upfront identification of the top payers, Brown notes, she also works with the billing department to trend denials. That report often determines what the next training focus will be. "If a certain number [of denials] are related to Blue Cross Blue Shield, we need to do some education on [that payer] this month."

Each time the department goes through the cycle of trending denials, educating with tip sheets, and checking for quality, she says, "we get a little bit better."

Registration errors have been reduced by more than half, Brown says, specifically those errors that lead to denials. "For example, a [wrong] patient address does not cause a denial."

"We found that when we focused on [cutting denial-causing errors], it increased overall accuracy as well," she adds.

Employee recognition enhances quality

Annual recognition for employees who excel in claim accuracy has been another important part of the quality focus, Brown points out. Those who score 90% or above on claim accuracy — meaning at least 90% of the claims they process are not denied — receive a gold medal, she says. An accuracy rate of between 85% and 90% earns a silver medal, and a rate of 80% to 85% earns a bronze medal, Brown adds.

"Right after we [awarded medals]," she notes, "everyone — the entire team — jumped to 90%."

"It was a great year for access last year," Brown says. "We got written up in the hospital newsletter, and the staff was treated to a party and received [commendation] letters. A lot of times access people complain about not being recognized, but we can't say that."

The recognition and sense of accomplishment not only has boosted staff morale, she adds, but has made the access department a more sought after place to work. "We have a lot more applicants, people wanting to be part of our team."

[Editor's note: Millie Brown can be reached at (404) 929-7514 or by e-mail at millie.brown@choa.org.] ■

Efficiency, not speed, counts most, experts say

AR days no longer the best benchmark

By **Craig S. Weller**, RHIA, MBA
and **Linda Fotheringill**, Esq.
Fotheringill & Wade Consulting, LLC
Baltimore

Almost every aspect of health care has changed significantly over the last five years, let alone the past 30. Most of us can remember when protecting a patient's privacy was an ethical issue for hospitals and physicians. Now it's a matter of regulatory requirement under the Health Insurance Portability and Accountability Act.

Beyond this recent change, however, there is an amalgam of activities that has had and will continue to have a profound effect on hospital financial viability. We have experienced cyclic problems with shortages of various professionals, access to affordable liability insurance, and the lack of capital for replacement of plant, equipment, and technology.

30% reimbursement comes from MCOs

Where hospitals once received 95% of their reimbursement from fee for service insurance companies, approximately 30% now comes from managed care organizations. Medicare and Medicaid, which were considered reasonable payers (low but steady), have fallen victim to budget cuts.

The Balanced Budget Act of 1997 completely changed the reimbursement scenario, and it is

estimated that additional reductions in Medicare payment may reach $21 billion in a five-year period. State governments are reducing programs, services, and funding for Medicaid recipients to avoid spending money that doesn't exist.

At the same time, the economic cycle has placed a burden on all companies to reduce costs, either to survive or enhance shareholder equity. This business reality is easily seen in the health care marketplace, where providers face a series of obstacles in getting paid for even the simplest of services. Internally, the "revenue cycle" most commonly is labor- and paper-intensive, with billing deadlines and collection goals.

Layered on top of this reality is a payer marketplace that can collect millions of dollars in interest by not paying claims on a timely basis. An even better result occurs if the claim is denied.

Between 25% and 30% of claims are denied

Industry estimates are that between 25% and 30% of all health care claims either are denied or rejected. With the economic climate and an increased market penetration of managed care, the number of denied claims continues to rise. The result is a direct threat to a hospital's financial viability.

This point was substantiated by Washington, DC-based The Advisory Board Co., a leading research organization, which recently surveyed hospital executives and found that decreased claim reimbursement is their highest-priority financial concern. In their responses, executives identified claim denials as the principal cause of the decreased claims reimbursement.

With all of the changes affecting health care, the basic measure used to compare hospital financial productivity has not changed. The venerable "days in accounts receivable [AR]" continues to be the choice for benchmarking one hospital against another. Unfortunately, many hospitals across the country live by this metric, even basing employee compensation changes on achievement of "days in AR" goals.

Financial policy can manipulate AR days

When examined under a bright light, it is clear that the number of AR days can be manipulated through financial policy. Some hospitals have policies that allow a write-off to bad debt for any denied claim under a defined value or over a certain age.

In the current environment, where every revenue dollar is important to future success, this criterion that once had universal appeal should now be viewed only as a measure of efficiency — how quickly did the hospital turn a bill into cash — and not a panacea for financial comparison. Perhaps more important is the establishment and regular reporting of a companion effectiveness metric — one that measures how well bills are turned into cash.

Scraping for every dollar

When the AR days measure became important to hospitals, claim denials were literally unheard of. Now, as we scrape for every dollar to meet both present and future needs, there must be an organizational commitment to identifying all denied and underpaid claims and aggressively pursuing a reversal of the insurer's determination.

Some hospitals have demonstrated leadership in creating multifunctional departments geared to protecting all aspects of the revenue cycle. They largely have been rewarded for their efforts by being more effective in their billing and collection practices. For everyone else, however, perhaps a low-tech solution to generating more cash for the hospital is a necessary first step.

Throughout the literature on modern management methods, examples can be found of improved performance when a process is measured and reported upon. Measuring and reporting both efficiency and effective metrics for financial operations will make clear the opportunity to turn denied claims into cash.

Hospital executives and board members need to understand the nature of the decreased claim reimbursement problem, as well as opportunities that exist within the organization for improving operations. Perhaps a good portion of our financial future is in our own hands — keep the money we have, and fight for what we deserve.

[Editor's note: Linda Fotheringill is a lawyer who frequently provides consulting services to hospitals in the area of denial management and is the co-author and a faculty member of the Denial Management Institute (DMI). Craig Weller is director of operations for Fotheringill & Wade and a faculty member of DMI. They can be reached at 212 Washington Ave., First Floor, Baltimore, MD 21204. Telephone: (800) 597-7759; Fax: (410) 296-1558; e-mail: l.fotheringill @fwhealthlaw.com.] ■

Looking for HIPAA help? Resource list may help

Being educated is the best defense when it comes to ensuring that your hospital is compliant with the requirements of the Health Insurance Portability and Accountability Act (HIPAA).

Liz Kehrer, CHAM, an experienced access manager who is now system administrator for patient access at Centegra Health System in McHenry, IL, is charged with the oversight of compliance and regulatory issues for her department.

During her research of HIPAA topics affecting access services, Kehrer compiled the following list of Internet resources, **below.** ■

HIPAA Internet Resources

Category	Description	URL
HIPAA	American Health Information Management Association	http://www.ahima.org/
HIPAA	American Hospital Association	http://www.hospitalconnect.com/aha/key_issues/hipaa/index.html
HIPAA	American Medical Association free brochure on "How to HIPAA"	http://www.ama-assn.org/ama/pub/category/8158.html
HIPAA	HCPro's-himinfo.com Contains resources and a free weekly newsletter	http://www.www.himinfo.com
HIPAA	HCPro's-HIPAA Weekly Advisor Archive	http://www.himinfo.com/hipaa_ezine/hipaa_arc.cfm
HIPAA	Illinois Hospital Association	http://www.ihatoday.org/public/hipaa/index.htm
HIPAA	Phoenix Health System HIPAA site contains various HIPAA explanations/resources	http://www.hipaadvisory.com
HIPAA Regulations	**HHS administrative simplification web site: Final & proposed regulations, guidance, FAA's**	http://www.aspe.hhs.gov/admnsimp/
Privacy	Georgetown University HIPAA site contains many resources including summary of state laws; health privacy	http://www.healthprivacy.org/
Privacy	Office of Civil Rights-Privacy web site	http://www.hhs.gov/ocr/hipaa/
Privacy	Summary of HIPAA: Privacy Rule, including 8/14/02 revisions	http://www.healthprivacy.org/usr_doc/RegSummary2002.pdf
Security	CPRI-HOST (Healthcare Security—Advancing Electronic Information Systems Security for Healthcare)	http://www.cpri-host.org/
Security	For the Record: Protecting Electronic Health Information	http://www.search.nap.edu/html/for/
Security	Nation Institute of Standards and Technology: Federal Agency Security Policies	http://www.csrc.nist.gov/fasp/
Security	Security Focus Online: Guide to Better Passwords	http://www.online.securityfocus.com/infocus/1537
Security	The SANS Security Policy Project	http://www.sans.org/newlook/resources/policies/policies.htm
Transactions	Standards Developing Organizations (SDO's) involved in HIPAA standard transactions & code sets	http://www.snip.wedi.org/public/articles/details.cfm?id=76
Transactions	Survey your software vendor's HIPAA readiness now	http://www.hipaadvisory.com/tech/HICI0101p1Reprt.pdf
Transactions	Washington Publishing Company web site (Contains implementation guides for the standard transactions)	http://www.wpc-edi.com/hipaa_40.asp
Transactions	Workgroup for Electronic Data Interchange-SNIP (Strategic National Implementation Process for HIPAA)	www.wedi.org

ACCESS FEEDBACK

'Free' hospital needs help sending payment message

Patients risk health with careless ID use

Nancy Stringer, director of patient access at Truman Medical Center in Kansas City, MO, would like to know how other nonprofit hospitals deal with the impact of nearby for-profit providers that have much stricter patient payment policies.

A large for-profit chain recently bought a group of hospitals in the Kansas City area, Stringer says, and she's concerned about what that will do to the balance of uncompensated care in the community.

Truman already is known as "the free hospital," she notes. "We always joke that the best marketing strategy our CEO could have would be to run a big ad saying that Truman isn't free. People think that just because we're a public hospital, they should be able to come and receive all the care they need without paying for it."

Exacerbating the situation has been a change at another Kansas City hospital, Stringer says. "It used to be primarily state-funded, but while it's still not-for-profit, it has changed its philosophy. [That hospital] is asking for cash up front; and when people are not able to do that, they come to Truman."

Her registrars constantly are dealing with people who can't afford to pay, who are anxious about getting help, but who, in many cases, don't qualify for Medicaid or other forms of aid, she says. "We have discounted care, but a lot of patients we see don't fall into our catchment area and aren't eligible for that."

Staff must tell these patients that while the hospital will continue to treat them, it also will continue to bill them, and to go through the collection process if necessary, Stringer explains.

"My big issue with all this is that I'm trying to make the workplace as pleasant as possible, and that's difficult to do when every other patient is anxious about how they're going to pay for care," she adds. "What I'd like to do is help my employees understand how to communicate with patients about these things."

Identifying patients

Another issue on which Stringer would like feedback from her access peers has to do with the proper identification of patients. While she's looking at technology options provided by health care vendors, one of the main problems is that many patients don't understand how not correctly identifying themselves can impact their health, Stringer points out.

"We still have cousins who use each other's IDs and [foreign] patients who share their visas," she notes. "One registrar asked for identification and the male patient showed the ID of a female friend. When the registrar said she needed *his* ID, the patient responded, 'Well, she told me I could use it.'"

In many cases, Stringer says, the problem is that patients don't have a good grasp of English or of how the health care system works.

"It's really a patient safety issue," she says. "We're not going to deny care if a person coming into the emergency department doesn't have a picture ID, but we need to have the correct health history and blood type. We want to make sure we've got the correct person."

Stringer also is hearing from her staff that people of certain nationalities either don't know their birth dates or use them in a different way. "They're all Jan. 1."

"Also, since [foreign] names aren't familiar to employees, if they're similar they sometimes don't recognize the difference," she adds. "It's enough of a problem that it poses a daily challenge."

The hospital has put together a multidisciplinary team, with representation from the legal department, to brainstorm solutions, Stringer says, but she would welcome suggestions from other access professionals.

Deliberate misidentification

Dee Alugbin, collections coordinator in patient access services at St. Joseph's Hospital of Atlanta, seeks help on a related issue — how to address the problem of deliberate misidentification.

St. Joseph's has many self-pay patients who deliberately give emergency department (ED) registrars the wrong information, she says. "When we try to call later in reference to their

admission and to work out a payment plan, we find out the telephone number is wrong, the address is wrong, and sometimes a number or two is off in the Social Security number."

"Is there a way we can cut down on that?" wonders Alugbin. She adds that she was unable to find solutions for this particular problem at the recent National Association for Healthcare Access Management conference, where other access professionals reported having similar experiences.

Tweaking collections

Although ED operations remain a major challenge, she has had some success in improving collections efforts in other patient access areas, as well as in the hospital's ancillary departments, says Alugbin, who was hired as collections coordinator in November 2002 and began working full time at the position in May 2003.

"I've been working all the different departments, just seeing what they do every day," she notes.

Alugbin says she recently observed registration activity in the Breast Health Center, where employees did not ask patients for copayments, even though in most cases the copay information is right on the insurance card.

"I just got a little sign saying, 'Copay is required at the time of service,'" she adds, and collections improved.

One of her initiatives has been to make copies of the insurance cards the hospital deals with most frequently, blocking out the patient's name and highlighting with a yellow marker the area where copay instructions are given, Alugbin says. "If the card doesn't give the copay information, I have them look up [that payer]."

If patients become argumentative when asked to pay, she notes, staff are instructed to explain that it is a new procedure, that they can be billed, but that it is better if they pay at the time of service.

At the hospital's Center for Wellness and Rehabilitation, the only ancillary area that is located several miles from the hospital complex, staff were reluctant to accept cash payments for security reasons, she says. They didn't want to keep large amounts of money on hand between visits to the main campus.

Noting that the bank the hospital uses has a branch right behind the center, Alugbin made arrangements to have employees make a deposit there every day. They simply keep the deposit receipts, she adds, and take them to the hospital cashier twice a month.

[Editor's note: If you have feedback on any of these issues or comments or information to share regarding any access topic, please contact editor Lila Moore at (520) 299-8730 or by e-mail at lilamoore@mindspring.com.] ■

JCAHO drafts standard for ED overcrowding

The Joint Commission on Accreditation of Healthcare Organizations (JCAHO) has released a proposed leadership standard on emergency department overcrowding.

The proposed standard calls on hospital leaders to develop and implement plans to identify and mitigate situations that result in emergency department (ED) crowding. It looks, for example, at whether hospital leaders incorporate ED crowding into performance improvement activities, coordinate with community resources such as home health agencies and long-term care facilities to expedite discharges from the ED, and use performance measures to monitor the capacity of support services and treatment areas that receive ED patients.

If approved, the standard would be implemented in January 2004. The draft standard is at www.jcaho.org. ▼

Hospitals picked for ED crowding program

Ten hospital systems have been selected to participate in a national initiative by the Princeton, NJ-based Robert Wood Johnson Foundation to reduce emergency department (ED) crowding and assess the health care safety net.

The health systems will receive up to $125,000 to develop and implement strategies to relieve

ED crowding, and will produce a report depicting the state of the safety net in their community. Four of the health systems also will receive $250,000 to implement specific demonstration projects.

Lessons learned from what is being called the Urgent Matters project will be disseminated to hospitals and communities nationwide. For more information and a list of participants, go to www.urgentmatters.org. ▼

Web site offers providers EDI implementation dates

The Workgroup for Electronic Data Interchange and the Council for Affordable Quality Healthcare have created a web site where providers can get health plan and clearinghouse schedules for testing and implementing electronic transactions standards under the Health Insurance Portability and Accountability Act (HIPAA).

Some participating health plans also provide a link to their HIPAA companion guides. The web site, aimed at helping providers plan for the rule's October implementation deadline, is at www.wedi.org/snip/caqhimptools. ▼

CMS proposes its new Medicare payment rules

The Centers for Medicare & Medicaid Services (CMS) has released its proposed rule for inpatient Medicare payments for fiscal year (FY) 2004.

Among the key items in the nearly 1,000-page rule are the following:

• CMS has calculated the market basket's increase in the cost of care to be 3.5% for FY 2004. However, due to budget neutrality and other adjustments, average payments to hospitals will rise only by 2.5%.

• The rule expands the post-acute care transfer policy to an additional 19 diagnosis-related groups. In an article by the on-line news service *AHA News Now,* the American Hospital Association (AHA) states that the estimated loss to hospitals would be $160 million in FY 2004.

• The rule raises the outlier threshold for extremely high-cost cases to $50,645 from $33,560. AHA said it expects a separate outlier rule soon from CMS that will contain adjustments expected to reduce that threshold. The rule is on the CMS web site at www.cms.org. ▼

Ft. Lauderdale site of Sept. AAHAM conference

The American Association of Healthcare Administrative Management (AAHAM) is holding its Annual National Institute (ANI) Sept. 25-27 at the Marriott's Harbor Beach Resort & Spa in Ft. Lauderdale.

AAHAM has co-hosted a conference with the National Association of Healthcare Access Management in the past and often addresses issues of interest to access managers.

For more on program topics and other ANI information, go to the organization's web site at www.aaham.org. ▼

More hospitals permitting family during procedures

About half the hospitals surveyed for a recent study allow family members to be present during emergency procedures, but only 5% have written policies to that effect.

About one-fourth of nurses responding to a survey by the American Association of Critical-Care Nurses and the Emergency Nurses Association reported that family presence was prohibited

COMING IN FUTURE MONTHS

- Tips on handling ABNs
- Is reimbursement on the way for illegal alien care?
- Revamping outpatient registration
- ED collection case studies
- Help with HIPAA's security rule

for cardiopulmonary resuscitation and invasive procedures, even though their units had no written policies prohibiting such access.

The nurses said family members asked to be present about one-third of the time for resuscitation and about two-thirds of the time for invasive procedures.

The trend is that more and more hospitals are allowing family members access during emergency procedures, according to the American Hospital Association.

The survey is reported in the May 2003 issue of the *American Journal of Critical Care* and the June issue of the *Journal of Emergency Nursing.* ▼

ED visits up 20% since '92, CDC says

Visits to U.S. hospital emergency departments (EDs) have climbed 20% in the past decade, according to a recent report by the Centers for Disease Control and Prevention (CDC) in Atlanta.

EDs received an estimated 107.5 million visits in 2001, about 17.5 million or 20% more than in 1992, the agency's latest annual National Hospital Ambulatory Medical Care Survey shows.

The CDC attributes the increase in part to U.S. population growth and an increase in older adults, who tend to visit EDs more often than younger people. The number of U.S. EDs also decreased by about 15% during the same period, the agency notes.

Hospitals in metropolitan areas and those affiliated with medical schools tended to have a larger volume of ED visits. Abdominal pain, chest pain, and fever were the most common principal reasons for visits. About 30% of ED patients had elevated blood pressure, and about one in four patients received medications during their visit.

For a summary of the survey findings, visit www.cdc.gov/nchs. ■

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

THOMSON
AMERICAN HEALTH CONSULTANTS

IN THIS ISSUE

JULY/AUGUST 2003
VOL. 1, NO. 4 • (pages 25-32)

Surveys gauge current state of HIPAA compliance

HIMSS, OIG release results of separate surveys

Now that two significant HIPAA compliance deadlines have passed — the April 14 deadline for health care industry compliance with the privacy rule and the April 16 deadline for health care business operations to begin testing transactions and code sets — it's time to take stock of how far along health care organizations really are when it comes to HIPAA compliance. To that end, both the Department of Health and Human Services' Office of Inspector General (OIG) and Healthcare Information Management Systems Society (HIMSS) have conducted surveys of health care providers.

HIMSS and Phoenix Health Systems conducted the HIMSS Spring 2003 HIPAA Survey. Among its findings are the following:

• 78% of providers, 68% of payers, and 47% of clearinghouses said they were compliant with the April 14 privacy deadline.

• Nearly 100% of providers who reported being privacy-compliant have implemented the most publicly visible elements of the privacy rule such as Notices of Privacy Practices and Patient Authorizations. However, significantly fewer have implemented requirements such as enabling patients to receive an accounting of health information disclosures, limiting staff access to protected health information on a minimum necessary basis, and completing agreements with business associates to ensure that they are protecting patient privacy.

• Among health care computer system vendors, only 39% had completed privacy remediation efforts.

• Cooperation among health care industry segments reportedly was less than satisfactory and again was ranked one of the top roadblocks to HIPAA compliance, along with "not enough time" and difficulty interpreting the HIPAA regulations.

• Management support for HIPAA compliance has significantly increased over measurements recorded in past surveys.

In-depth reports

Looking at privacy compliance in more depth, HIMSS reports that some 98% of reportedly compliant providers have implemented the most publicly visible requirements, such as the Notice of Privacy Practices, obtaining patient acknowledgement of receipt of the notice, and obtaining patient authorizations for use and disclosure of protected

health information. But only 88% have put in place other requirements, such as a process for providing an accounting of disclosures to patients, or setting minimum-necessary protected health information access restrictions on health care workers.

Forty percent of "compliant" providers indicated they had not yet finalized business associate agreements that will ensure that business partners with access to protected health information are protecting patient privacy. Twenty-nine percent have not implemented a working process for monitoring privacy compliance, and 18% do not yet have the privacy rule's required data security protections in place.

A more intense look at the transaction and code set compliance report suggested to HIMSS that on-time implementation of the highly visible privacy regulations may have dominated the focus of health care HIPAA compliance efforts in recent months. That emphasis may have delayed transactions and code sets compliance efforts in many health care enterprises, especially provider organizations.

In this survey, only one-half of all participants reported completing of transaction and code sets implementation activities, and just 53% had begun internal testing by the April 16 deadline. Still, a majority of organizations had completed transaction and code sets HIPAA awareness/education (78%), assessment (73%), and implementation project planning (67%). Further, almost 40% of respondents already had begun external testing with business partners.

Internal transaction testing was being conducted by 49% of all providers, 62% of payers, 55% of vendors, and 80% of clearinghouses as of the April 16 testing deadline. Only 39% of providers, 37% of payers, 39% of vendors, and 53% of clearinghouses were conducting external testing with their trading partners as of the testing deadline.

Spring 2003 survey results showed that 44% of respondents across the industry were using outside consultants to support HIPAA initiatives. As in the past, the biggest users of consultants were larger hospitals (46%) and payers (66%). Approximately 30% of respondents engaged consultants for assessment and implementation planning services, 22% for implementation support, and about 45% for HIPAA awareness and training support.

Hospital budgets for HIPAA compliance in 2003 generally are higher than 2002 HIPAA budgets. Also, payer budgets for 2003 are significantly higher than in 2002, especially for larger payer organizations.

Part A readiness

Meanwhile, OIG's report used a mail survey of Medicare Part A providers to assess level of readiness in four broad areas — assessment and awareness activities, impediments or current obstacles to achieving compliance, compliance strategies such as sequencing and testing plans, and contingency planning.

OIG says that almost all Part A providers have submitted a compliance extension form giving them until Oct. 16, 2003, to implement electronic standards and code sets. At the time of the OIG survey, 74% of providers were ready to implement the HIPAA electronic standards, and 96% indicated that they had a moderate to high level of satisfaction that they expected to meet the October deadline.

The 4% of providers not expecting to meet the compliance deadline said they were in the process

HIPAA Regulatory Alert (ISSN 1542-9830) is published bimonthly by Thomson American Health Consultants, 3525 Piedmont Road, Building Six, Suite 400, Atlanta, GA 30305. Telephone: (404) 262-7436. Periodicals postage paid at Atlanta, GA 30304. POSTMASTER: Send address changes to **HIPAA Regulatory Alert**, P.O. Box 740059, Atlanta, GA 30374.

Subscriber Information

Customer Service: (800) 688-2421 or fax (800) 284-3291. Hours of operation: 8:30-6. Monday-Thursday, 8:30-4:30 Friday EST. World Wide Web: http://www.ahcpub.com. E-mail: customerservice@ahcpub.com.

Subscription rates: Free to subscribers of *Healthcare Risk Management* and *Hospital Access Management*. For nonsubscribers, the price is $149. U.S. possession and Canada, add $30 plus applicable GST. Other international orders, add $30. (GST registration number R128870672.) 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 $48 each.

Editor: **John G. Hope**, (717) 238-5990.
Managing Editor: **Russ Underwood**, (404) 262-5521.
Vice President/Group Publisher: **Brenda Mooney**, (404) 262-5403, (brenda.mooney@ahcpub.com).
Editorial Group Head: **Coles McKagen**, (404) 262-5420, (coles.mckagen@ahcpub.com).
Production Editor: **Nancy McCreary.**

Editorial Questions

For questions or comments, call **Russ Underwood** at (404) 262-5521.

of identifying the steps necessary to implement the standards.

While fewer than 30% of the providers had begun any testing, 90% will have a testing strategy. Most of the testing strategies include internal and external data interfaces. About 25% had begun to test transactions as of November 2002. However, only slightly more than 44% had received any notices from fiscal intermediaries or carriers regarding coordination of electronic transaction testing.

Strategies and barriers

When asked which strategy providers were using to implement the HIPAA standards, they most frequently identified these four: internal staff planning, developing, and implementing the standards; technical systems consultants working with staff and assisting in the process; technical systems consultants or vendors taking full responsibility for planning, developing, and implementing standards; and purchasing components of a new system or additions to current systems from a selected vendor to meet the standards.

Likewise, when asked to list as many as three barriers to compliance, 60% of the respondents listed one or more. The most common were: trading partners will not be ready; vendors will not be ready; inadequate staffing, training, and technical resources; and not enough time to implement.

One-third of those who listed any barriers identified their trading partners (specifically third-party payers, fiscal intermediaries, and / or the Centers for Medicare & Medicaid Services) as potential barriers to compliance. Providers who did not believe they would meet the compliance deadline expressed similar concerns. They cited their trading partners as a potential barrier, as well as inadequate resources.

More information is available from www.hipaadvisory.com. ■

Popular PC applications can cause security leaks

Is instant messaging compromising your PHI?

A report issued by Palisades Systems Inc. in Ames, IA, and Clive, IA-based HIPAA Academy, says that health care organizations that allow peer-to-peer (P2P) and instant messenger applications to run on their computer networks risk compromising patient health information and causing HIPAA privacy violations.

"P2P applications open up a health care organization's network to the outside world," says HIPAA Academy compliance manager **Mark Glowacki**. "Applications like P2P and instant messenger allow employees to communicate and share files covertly with outside parties. Because these applications can run without being detected by conventional security applications like firewalls, security violations are only discovered after the fact. With instant messaging, undocumented communications regarding a patient may occur without the health care organization's knowledge, leading to an unintentional breach of HIPAA's access requirements."

In addition to undetected file sharing, P2P and instant messenger can expose an organization to security threats targeted at these applications, such as worms, viruses, and spyware. Glowacki says that several P2P applications include spyware as a standard part of the installation, which may allow for unauthorized collection and distribution of confidential information. Free instant messaging applications can allow a hacker to take over the user's computer through security vulnerabilities that are not actively patched.

Police department passwords found

According to the report, in September 2002, Aspen, CO, city government officials received an e-mail indicating that someone had downloaded police department passwords and sensitive city information from its network through a file-sharing program. The user was searching for a movie and came across the entire contents of the network administrator's hard drive.

According to the report, although some cases of sharing confidential information are malicious, most involve users who are not savvy enough to restrict access only to appropriate files.

The authors say that instant messaging applications provide no control over the sharing of confidential materials. Employees using such applications related to patients open an institution to critical information leaks that can be a breach of HIPAA security requirements. "It would be easy for employees to illegally share

critical protected health information with outside parties, either unintentionally or maliciously, without the detection or knowledge of the health care organization," the report declares. In addition, hackers can leverage well-documented instant messenger security vulnerabilities to take over computers.

"No organization with P2P or uncontrolled instant messenger programs running on its network can be HIPAA-compliant," says Palisade Systems president **Doug Jacobson**. "The applications open up too many security holes, and companies discover them too late."

For more information, go to www.palisadesys.com or www.hippaacademy.net. ■

Interim rule on monetary penalties to be replaced

Final enforcement rule to take effect Sept. 16

The Department of Health and Human Services (HHS) says its interim final rule establishing rules of procedure for the imposition of civil monetary penalties on entities that violate standards adopted under the administrative simplification provisions of HIPAA will not be in effect after Sept. 16, 2003, because it will be replaced by a final enforcement rule.

HIPAA gives the HHS Secretary of Health and Human Services the authority to impose a penalty of not more than $100 for each violation of a provision of the administrative services sections up to a yearly maximum of $25,000 for all violations of an identical requirement or prohibition.

The law says the secretary cannot impose a civil monetary penalty if: 1) it's for any action that can be punished under the law's criminal penalty provisions; 2) it is established that the person liable for the penalty did not know that a provision was being violated; 3) the failure to comply was due to a reasonable cause and not willful neglect; and 4) payment of the civil monetary penalty would be excessive relative to the compliance failure involved.

The department notice says its approach to enforcement is to seek and promote voluntary compliance with HIPAA provisions. The agency is offering technical assistance to promote voluntary compliance. Enforcement activities will be primarily complaint driven and will consist of progressive steps that give an opportunity to demonstrate compliance or submit a corrective action plan.

The interim final rule discusses all the procedures involved in imposition of civil monetary penalties.

To download the interim final rule, go to www.cms.gov/hipaa/hipaa2/enforcement/default.asp#penalties. ■

HIPAA affects ability to help law enforcement

Specific HIPAA provisions still must be followed

When two police officers arrived at a hospital emergency department asking to be informed if the facility had treated an elderly woman reported missing by her family, hospital staff contacted their outside legal counsel for advice because of wariness about HIPAA privacy regulations. And it's good they did.

Nixon, Peabody attorney **Claudia Hinrichsen**, who is leading the Garden City, NY, firm's HIPAA practice, says there are specific HIPAA provisions relating to release of information to law enforcement officials that must be followed, no matter how much staff may want to help the police do their job.

In the instance cited above, the woman had been treated at the hospital and specifically informed the hospital staff that she was planning to enter a particular nursing home but that her family was not to be informed of her location.

While the staff were eager to allay the family's fears and assist the police, they were faced with HIPAA restrictions on the information they could disclose. HIPAA describes the types of information that can be provided to law enforcement officials who are looking for a fugitive, a suspect, a material witness, or a missing person.

Competing restraints in state law

Complicating the issue in this instance was the fact that New York State has its own laws on cooperating with law enforcement, so that there were competing restraints. Generally in the past, it has taken a court order to free a hospital to disclose information.

Hinrichsen says she advised the hospital to

indicate that staff were not at liberty to disclose the woman's location. The most the hospital could have released, she said, was information such as name and address, Social Security number, and date of treatment at the hospital.

"My general guidance to facilities is to have a policy in place about disclosure of protected information to law enforcement officials," Hinrichsen says. "The policy should deal with the specific requirements in Section 164.512(f). It also should consider any more restrictive state laws for the particular state in question."

She tells of a hospital that traditionally notified the local police automatically whenever someone was treated for injuries resulting from a traffic accident. However, it was determined that there is no specific authorization for releasing such information and the hospital was advised to change its practice.

Hinrichsen says that hospital staff members accustomed to cooperating with the police may feel uncomfortable in saying that they cannot give out information any longer, but that still may be the only correct response and the one that should be used. She said they can always offer to pass the issue on to the hospital attorney or to an administrator to handle.

For more information, contact Hinrichsen at (516) 832-7532. ■

Company develops business associate agreement

Template created to fulfill HIPAA requirements

One of the nation's leading medical messaging services has taken the lead in developing a sound business associate agreement to present to its clients to fulfill HIPAA requirements.

Long Island, NY-based MEDFONE Inc., which works strictly for health care clients such as group practices, individual physicians, and insurance companies, offering them medical messaging services such as an answering service, telemarketing sales, and inbound and outbound call center activities, drew up a proposed business associate agreement template once president **Jay Moses** realized how much work would be involved in reviewing the wide variety of agreements being received from clients.

"We process 10,000 calls a day for more than 800 clients nationwide," Moses tells *HIPAA Regulatory Alert*. "Many of these calls deal with patient health information. We were already very security conscious, but we had to upgrade our technology platform to ensure that all calls are encrypted, safe, and password-protected. And we've trained all of our agents in what it means to be HIPAA-compliant."

Moses tells us that by the time he had received 200 business associate agreements from customers, he realized that HIPAA was going to be a huge undertaking for his organization, and also that many of his clients really did not have a good understanding of what HIPAA meant.

Template drafted

As a result, Moses turned to his company's outside law firm to draft a business associate agreement that he could send to clients on his own initiative. While it was a voluntary service he offered, many of the clients went ahead and used them, he says, freeing time for him and his law firm because he knows that when one of his agreements comes back, it will be acceptable without extensive review.

Moses says that MEDFONE, which recently won an award of excellence from *Customer Interactive Solutions* magazine, has never had a confidentiality problem in the 25 years in which it has been in business. "It's in the nature of our business that we already had many safeguards in place," he says. "But we still had to go to some very expensive changes to be sure that we would meet all requirements for our clients."

Moses says that because MEDFONE is required to store files for no less than six years, he had to upgrade storage devices, using a combination of on-site and off-site storage.

Asked his assessment of HIPAA readiness in health care covered entities based on contacts made with him, Moses expressed concern that HIPAA may still be an unknown entity for many organizations. "We still don't know what the repercussions will be if an issue arises," he says. "There are no HIPAA police out there and no legal precedents. Some people say HIPAA is like Y2K — lots of hype and not much else. We'll know more in October. We need to be able to handle the encryption keys that our clients need us to use. Because there's no standardization — and, really, standardization is almost contrary to what HIPAA is trying to accomplish — we're going to have to be able to deal with many different

encryption systems. It's important for our clients to know that they can work with us and we've done our due diligence. We don't want any of our clients or ourselves to be liable if an issue arises."

Moses says it's important that people realize HIPAA came about out of a desire for the financial savings for Medicare that can come from processing data in a consistent format. Health care organizations have to realize that there is a tremendous liability with penalties that can be severe, he says. He indicates that MEDFONE realizes that providers want to practice medicine and not worry excessively about administrative things, and that's why his company's role is to free clients as much as possible to concentrate on providing care.

For more information, contact Moses at (516) 679-7629. ■

WEDI seeks transaction and code set guidance

Concerns over the compliance of trading partners

The Workgroup for Electronic Data Interchange (WEDI) has asked Health and Human Services Secretary **Tommy Thompson** to provide guidance in light of the fact that a substantial number of covered entities will not be able to achieve compliance with HIPAA Transaction and Code Set (TCS) standards by Oct. 16, 2003, as required under the Administrative Simplification Compliance Act.

In a letter to Thompson, WEDI reported that a number of covered entities that will be compliant are worried about trading partners or transactions that will not be compliant. The covered entities are considering contingency plans to avoid unintended consequences and adverse impacts, including rejection of nonstandard electronic transactions; disruption of payment flows to providers under Medicare, Medicaid, and private-sector health plans; and reversion to paper transactions by covered entities that are capable of generating transactions in a nonstandard format.

WEDI said that much progress has been made and there is considerable industry support for HIPAA TCS standards and their successful implementation. "The issue at hand," the group said, "is how does the industry make the short-term transition from its current state to a successful implementation, given a substantial degree of noncompliance in October 2003, and thus avoid the so-called train wreck that will result from reversion to paper claims or stoppage of cash payment flows."

Potential solutions offered

Two potential solutions the group asked Thompson to consider were 1) permitting compliant entities to use HIPAA TCS standard transactions that may not contain all required data content elements, if these transactions can otherwise be processed to completion by the receiving entity, until such time as compliance is achieved or penalties are assessed, and 2) permitting compliant covered entities to establish a brief transition period to continue using their current electronic transactions in lieu of reversion to paper transactions.

WEDI said its experts believe that reversion to paper has the highest potential for unintended consequences and adverse impacts for the health care industry. It indicated that its two recommended courses of action would not have an adverse impact on compliant covered entities.

"Further," WEDI says, "they eliminate the need for covered entities that are in the process of achieving but will not achieve HIPAA TCS standards compliance by the deadline from diverting scarce resources to reverting to paper as a temporary fix to avoid noncompliance. The choice to accept a nonstandard electronic transaction would be at the discretion of the covered entity. Nothing would compel a covered entity to forego its rights or obligations, nor would it preclude a compliant covered entity from filing complaints with the Centers for Medicare & Medicaid (CMS). In fact, WEDI contends that CMS' complaint-based enforcement approach will be an incentive to hasten compliance with HIPAA TCS standards transactions, as will competition in the health care marketplace."

The group told Thompson that the health care industry believes that the goals underpinning a successful implementation of HIPAA TCS standards are to sustain cash flows from payers to providers, to minimize disruptions to business activities in the health care industry, and to allow sufficient time for covered entities that are making the effort to comply with HIPAA TCS standards transactions to make the transition to a successful implementation.

"For example," the letter says, "a large clearinghouse that is now compliant with the HIPAA TCS standards indicates that it has completed testing with only about 10% of more than 1,000 payers, and that it will not be able to complete testing by Oct. 16, because it is having difficulty with its payers scheduling testing because of the payers' time constraints. Industry participants have indicated that a transition of approximately six months should be sufficient to achieve critical mass for a successful implementation."

For more information, visit www.wedi.org. ■

Software can ease authorization process

Electronic records keep facilities connected

As with many areas of health care, new approaches in technology have been sought to ease the way into compliance with HIPAA. One example is the HIPAA GUARD program from Monterey, CA-based Integritas Inc.

The program, which can be used either as a stand-alone or in concert with the STIX occupational health suite, was created in anticipation of the new HIPAA requirements, says **Mary Stroupe**, MA, MBA, vice president of sales for Integritas.

"We anticipated it would be needed," says Stroupe. "We were clear that HIPAA was going to apply to all our clients — both to freestanding occupational health and rehab organizations, and in the hospital-based environment, where we see an even greater need."

Authorization is the linchpin

While HIPAA GUARD addresses a number of concerns, including privacy notice acknowledgement and consents, authorizations, patient access requests, patient complaints, and accounting of disclosures, patient authorizations seemed to be an overriding concern for a number of clients. "Fundamentally, we saw that according to the law as we read it, the release of information to the employer for the purpose of a physical or a drug screening would require an authorization from the patient," Stroupe explains. "In a health system, if you go to three or four different places, should you have to be given three or four different privacy agreements? In the scheme of all issues, that's No. 1."

Evelyn S. Miller, CPA, executive vice president-finance for Medway Health Inc. in Dallas, agrees. "You don't want it to look to your clients like you don't know what you're doing," she notes. "If they come into your clinic and sign a privacy agreement, then get referred to the hospital, which is owned by the same company [and get asked to sign another], they think you are clueless."

Miller has just such a situation. "We have two freestanding locations, each with three distinct treatment departments," she says. "It's helpful for us to know whether a patient has already signed an authorization form; it not only eliminates paperwork, but we are perceived as being more professional." Miller says this is one of the primary reasons she decided to integrate HIPAA GUARD with her STIX software.

There are other reasons managing HIPAA compliance with software can be beneficial. "We anticipate that whether you are a freestanding facility or a hospital, because the occ-med department is the department that routinely releases information to the employer, this could potentially be a source of weakness in the whole system," notes Stroupe. "Plus, even though the law does not require authorization for purposes of workers' comp, it *does* require you to document and keep track of disclosures made for workers' comp. If you're a small operation, you can just pull out the chart and see it; but in a large one, where you have many disclosures in many different places, having no single place to keep track of all of them is a huge problem."

Miller sees other reasons for the electronic record keeping the software facilitates. "When we get audited, surveyors want to see your compliance with HIPAA and how you track it," she notes. "We are getting ready for our accreditation by CARF [the Commission on Accreditation of Rehabilitation Facilities], and they want to see how we are complying with HIPAA, as well as logs of where we have done the accounting, whether people are receiving proper notice, and so on."

Not a performance change

Both Stroupe and Miller agree that the new Privacy Standard may change the way certain processes are handled, but not the way care is given.

"The general thinking is that HIPAA allows health care providers to do things that in the past they couldn't do, but that's just not true," Stroupe

asserts. "It requires providers to tell people what is happening. What I anticipate is this: in the past, patients haven't asked to see their records; and in most cases, it probably never occurred to them to ask.

"Now they're being given a document that tells them there's a new law that says what their rights are," she continues. "Soon, a certain percentage of people will start to request their records just because they can. This can cause real headaches, because the law requires you to reply to these requests within a certain amount of time. The software keeps track of when this has been done, what is pending, and so on. Even in the absence of any breach this is important."

"I agree," says Miller. "We've not yet seen any increase in the number of requests for medical records. We already had a response system in place; this is just making it more standardized. Basically, for us, it's just creating more work to document what we already do."

[For more information, contact:

• ***Evelyn S. Miller**, CPA, Executive Vice President-Finance, Medway Health Inc., 2915 LBJ Freeway, Suite 102, Dallas, TX 75234. Telephone: (972) 241-9271. E-mail: evelynmiller@medwayhealth.com.*

• ***Mary Stroupe**, MA, MBA, Vice President-Sales, Integritas Inc., 2600 Garden Road, Suite 112, Monterey, CA 93940. Telephone: (800) 473-6309.* ■

Companies seek URAC security accreditation

Ten companies operating in more than 20 different sites across the nation are in the process of seeking accreditation under URAC's HIPAA Security Accreditation Program for Covered Entities and Business Associates. URAC president **Gary Carneal** says the commitment to security shown by those who are seeking accreditation "sets an excellent example for covered entities and business associates alike."

With a strong emphasis on the fundamentals of ongoing risk management, URAC's HIPAA Security Accreditation program enables health care organizations to validate their security compliance program and demonstrate to their customers and business partners that they have taken the necessary steps to safeguard protected health information as required by the HIPAA security rule.

The companies seeking accreditation include American Specialty Health, Inc., and its affiliates, American Specialty Health Plans of California, American Specialty Health Networks, American Specialty Insurance Co., and Healthyroads; Health Ink & Vitality Communications; Imogen Systems; MedRisk Inc.; National Imaging Associates Inc.; and Wausau Benefits.

URAC HIPAA Security Accreditation is awarded for a two-year period, at the end of which an accredited organization must submit a reaccreditation application for URAC's review before accreditation is granted for an additional two-year periods.

More information on the program is available at www.urac.org. ▼

HIPAA.ICC.NET started to facilitate transmission

Internet Commerce Corp. says it has created a new service to address the need for health care payers and providers to exchange health care transactions that conform with HIPAA requirements. The new service, known as HIPAA.ICC.NET, incorporates software from eServices Corp. as well as that company's expertise in the new health care transaction requirements.

The company says that HIPAA.ICC.NET provides for seamless transmission of the HIPAA standard transactions between payers and providers.

"In today's health care environment, controlling costs is a major challenge," says ICC marketing vice president **Arnold Capstick**. "This new capability is aimed at providing a highly reliable, secure, accurate service at transaction prices that are more cost-effective than the current norm in the health care industry. HIPAA.ICC.NET allows users to comply with HIPAA regulations with a minimal investment of time and money." ■