Report on
PATIENT PRIVACY

Volume 7, Number 1 • January 2007

Practical News and Strategies for Complying With HIPAA Rules

Contents

Editor
Eve Collins

Contributing Editor
Nina Youngstrom

Executive Editor
James Gutman

Seeming Lack of OCR-DOJ Coordination On Complaints Hampers Enforcement Efforts

The HHS Office for Civil Rights says it has no real idea why the Department of Justice (DOJ) has failed to act on any of the privacy cases OCR has referred for possible criminal prosecution. That's because DOJ officials don't tell OCR why a case is closed; they just give notice that it has *been* closed, according to OCR.

Susan McAndrew, OCR senior advisor for health information privacy policy, made this startling statement in public comments before the National Committee on Vital and Health Statistics (NCVHS), a government advisory committee monitoring implementation of the privacy rule.

OCR is responsible for civil enforcement of the privacy rule, and DOJ is responsible for criminal. Since the rule took effect, DOJ negotiated three plea agreements for violations of the rule, but none were based on OCR-referred complaints. OCR has not imposed any fines, and both agencies are the subject of ongoing criticism. A new Democratic-controlled Congress is taking office this month for this first time since the rule was passed, and members are likely to hold oversight hearings as to why there has been no action by either agency *(RPP 12/06, p. 4)*.

At the meeting in late November, an NCVHS committee member asked McAndrew how OCR addresses allegations of lack of enforcement of the rule by either OCR or DOJ.

continued on p. 7

Patients Confused, Sometimes Suspicious About Rights to Accounting of Disclosures

This may be a familiar scenario at some hospitals: A patient requests an accounting of disclosures after receiving treatment in the emergency room, but when there are almost no entries on it, the patient is baffled — and suspicious the hospital is hiding something, especially since he knows for a fact that his medical records were sent for follow-up to his primary care physician.

As more patients at some hospitals capitalize on their right to see who is viewing their medical records, privacy officers say, these patients are startled to discover there are some big exceptions to the accounting-of-disclosures provision.

Then again, the above scenario may be alien to the hospitals that have still not received a single request for an accounting of disclosures. A number of hospitals say that patients have never exercised this HIPAA-endowed right, according to interviews with privacy officers. They're glad their facilities didn't sink fortunes into whiz-bang computer systems designed to log and centralize a patient's disclosures on request.

Either way, change is on the horizon in some respects: Some hospitals are getting more requests, and this is ushering in a bit of frustration and skepticism among patients who didn't realize the accounting-of-disclosures right was limited. Hospitals are responding to this by educating them and, in some cases, putting more disclosures on the accounting than HIPAA requires.

continued

According to Sec. 164.528 of the privacy regulation, patients have the right to an accounting of disclosures of their protected health information (PHI) within 60 days of submitting the request. Covered entities must produce a list of all PHI disclosed during the previous six years, with certain major exceptions (see flow chart, p. 3). The accounting does not have to include disclosures made for treatment, payment or operations (TPO) or disclosures authorized by the patients. And disclosures are not included if they are made for certain other reasons, such as national security or intelligence purposes and to correctional institutions or law enforcement officials.

So what does appear on an accounting? All sorts of disclosures, including births and deaths, disclosures to regulators (e.g., child and elder abuse reporting, disclosures for health fraud investigations, disclosures for research, FDA reporting for adverse drug events) and inadvertent disclosures (e.g., misdirected faxes).

Note the Lack of TPO Disclosures Up Front

Some hospitals see a trend toward more requests for accounting of disclosures, but "it's still in the trickle category," says Frank Ruelas, compliance officer for Iasis Healthcare Corp. in Tempe, Ariz. And there is a lot of misunderstanding about it.

Report on Patient Privacy (ISSN: 1539-6487) is published 12 times a year by Atlantic Information Services, Inc., 1100 17th Street, NW, Suite 300, Washington, D.C. 20036, 202-775-9008, www.AISHealth.com.

Editor, Eve Collins; Contributing Editor, Nina Youngstrom; Executive Editor, James Gutman; Publisher, Richard Biehl; Marketing Director, Donna Lawton; Fulfillment Manager, Laura Baida; Production Coordinator, Russell Roberts

Call Eve Collins at 1-800-521-4323 with story ideas for future issues of *RPP*.

Subscriptions to *RPP* include free e-mail delivery in addition to the print copy. To sign up, call AIS at 800-521-4323. E-mail recipients should whitelist **aisalert@aispub.com** to ensure delivery.

To order **Report on Patient Privacy**:

(1) Call 1-800-521-4323 (major credit cards accepted), or

(2) Order online at www.AISHealth.com, or

(3) Staple your business card to this form and mail it to:
AIS, 1100 17th St., NW, Suite 300, Wash., DC 20036.

Payment Enclosed* ❑ $363

Bill Me ❑ $388

*Make checks payable to Atlantic Information Services, Inc.
D.C. residents add 5.75% sales tax.

"When patients hear about the right to ask for an accounting and that it will list when the entity discloses PHI to another party, they figure any time a disclosure occurs, it will be listed on the accounting," he says. Obviously, they don't realize there are big exceptions.

The absence of information often makes patients assume the hospital made an error or is hiding something, Ruelas says. They may say, "I know for a fact you sent my [emergency department] records to my doctor's office. Did you make a mistake and not admit it?"

To minimize confusion, Ruelas has directed the staff members who generate an accounting of disclosures to add the following footnote in capital letters: "PLEASE NOTE: THIS ACCOUNTING OF DISCLOSURES MAY NOT LIST DISCLOSURES MADE FOR TREATMENT, PAYMENT OR OPERATIONS AS THEY RELATE TO YOUR MEDICAL OPERATIONS."

That way, patients who are in panic mode about the scarcity of entries on their accounting of disclosures will have an immediate explanation to calm them down. Then they can ask the privacy officer more questions to understand what's going on, Ruelas says.

Some Put TPO Disclosures on Accounting

Here's a twist: HIPAA doesn't require hospitals (and other covered entities) to put TPO disclosures on the accounting, but some hospitals include them anyway. "Some facilities will be very conservative, and some are very loose," says Ruelas, who has conducted his own survey of accounting-of-disclosures practices with 12 privacy officers.

Some use a checkbox system in their software so they can indicate which disclosures they want put in the accounting, he says. "Other [covered entities] will put every disclosure on the accounting of disclosures," he says.

And therein lies the rub: When patients have different experiences at different facilities, they may think the facility that is conforming to the HIPAA minimum is out of compliance.

The procedure for gathering disclosures at Iasis, Ruelas says, is "pretty sophisticated." Staff logs in every disclosure and notes what type it was (e.g., disclosure to Dr. Smith for treatment purposes, employer blood test, legal disclosure in response to a subpoena, disclosure to law enforcement). So Iasis's system starts to build a history of disclosures made about the patient, and when he or she comes in for the accounting, "the system will go back and pick up every disclosure not identified as TPO," Ruelas says.

But he has also seen hospitals successfully use simpler tracking systems for producing accounting of disclosures, such as Microsoft Excel spreadsheets.

Accounting Reveals Details

Cascade Healthcare Community (CHC) in Oregon, the parent company of two Oregon hospitals — St. Charles Medical Center-Bend and St. Charles Redmond — received only three requests for accountings of disclosures in 2006. Patients wanted to know who, among clinicians, was looking at their accounts.

"It's not so much a question of information being disclosed externally, but rather internally," said Judi Hofman, Cascade's privacy officer.

The limited number of disclosures on the accounting sometimes can trigger patient suspicion, Hofman says. "Most people's reports don't have a lot of activity," she says. In small communities like hers, many of the care providers know the patients personally or the patients know someone in another department, such as patient accounts or finance, "and sometimes a patient will become concerned about who internally has viewed their medical record," Hofman says. "That's where I come into the picture."

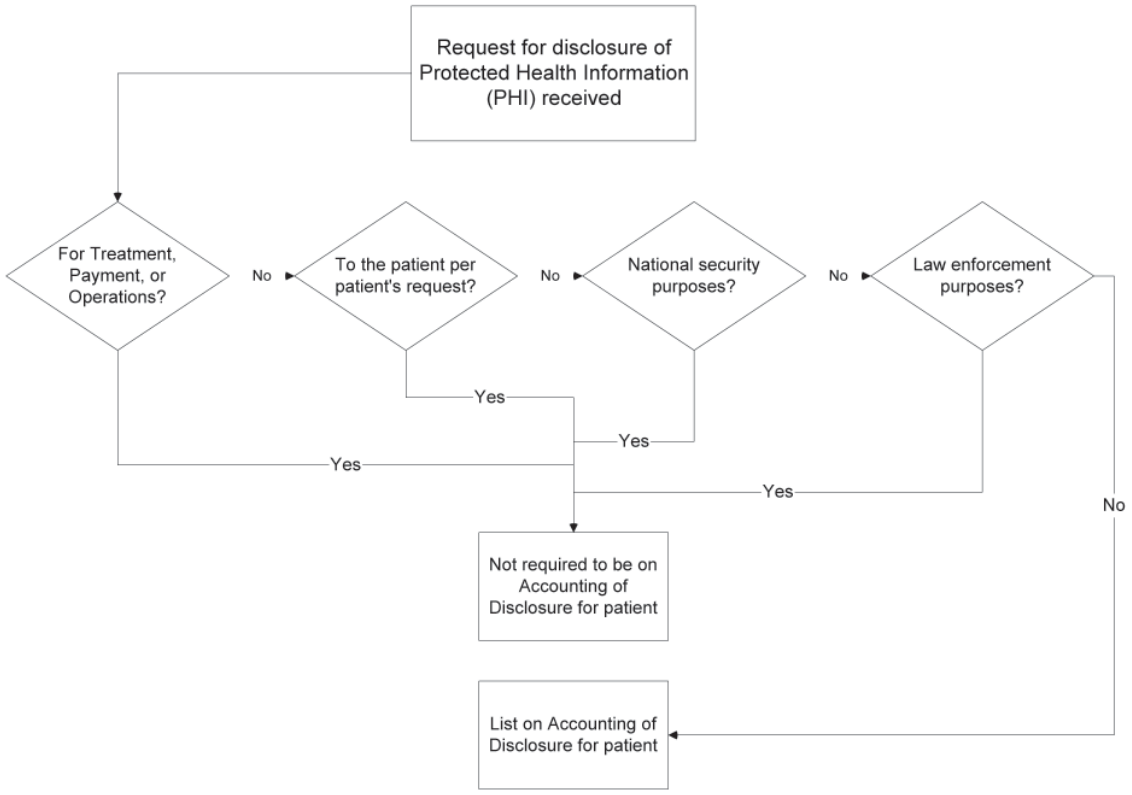
She investigates their concerns and confirms that their information has been disclosed properly — or otherwise. "We have really accurate audit trails of each person who has accessed a patient record," Hofman says. "If there happened to be a breach, and if we were able to confirm that with an investigation, that would be on the accounting."

Sometimes it may be a case where the patient has opted out of the directory but PHI was leaked to a family member. Hofman's breach investigational team, with the lead from the department director, will follow up with disciplinary action if it's warranted.

At CHC, the three accountings produced for patients had virtually nothing on them. Only one of three patients called Hofman back and said "I think someone was looking into my account." She says she will follow up with a probe if their concerns have legs, but first reiterates to the patient his or her rights under HIPAA. "Most people are pretty confused about their rights as patients. Once you start to spend some time explaining

Accounting-of-Disclosures Flow Chart

Here is a basic diagram that explains whether disclosures must be listed on an accounting of disclosures, according to the HIPAA privacy regulation. It was devised by Frank Ruelas, who is the compliance officer for Iasis Healthcare Corp. in Tempe, Ariz. Contact Ruelas at fruelas@iasishealthcare.com.



their rights as patients — that TPO disclosures won't show up on the accounting — they start to feel more comfortable," she says.

At Other End of the Spectrum

About half the privacy officers interviewed say that since the privacy rule took effect almost three years ago, they have not had a single request for an accounting of disclosures from a patient.

Case in point: Candace Foster, privacy officer at Deaconess Hospital in Evansville, Ind. Not a single request has come in for an accounting. Why don't patients ask for one? Foster assumes that when people ask about disclosures of their PHI, it's because they are concerned about a specific potential breach — "an incident in time" that may generate an investigation. Either an unauthorized access occurred, or it didn't. They don't want some general list from a long period of time, Foster says.

Also, she says, "I think a lot of people aren't aware" of their right to an accounting, even though it's mentioned in the notice of privacy practices (NPP). Most people "don't read the NPP," she says.

Foster has had patients (usually employee-patients) demand to know the identities of every person who has read the patient's medical records. But Foster turns them down. HIPAA does not require that — for clinical reasons, various nurses and physicians may have seen the patient's chart — and she does not grant those requests unless the patient has a credible reason to believe that one of the clinicians or another employee inappropriately accessed those records. She tells the patient that "I will investigate, but I will not give you a list of all the people who touched your medical records,'" Foster says.

If and when Deaconess ever gets a patient's request for an accounting of disclosures, here's the process: Foster and the medical records manager would review the patient's chart "to look for red flags suggesting an accounting should occur" (e.g., an emergency department chart shows a patient died and the hospital notified the Indiana organ procurement organization).

Based on the medical-record review, Foster says, every department that could have made a disclosure is asked to scour its records for the period for which the patient has requested an accounting. "We would make patients specify a period, or it will be very tedious to track down disclosures," Foster says. This includes departments like the pharmacy, radiology and cancer registrar. Then all the information is centralized.

Some Facilities Haven't Received Requests

Like Deaconess, other hospitals report a total absence of requests for accounting of disclosures since the HIPAA privacy regulation took effect in 2004. For instance, Ohio-based Catholic Healthcare Partners (CHP), which has 30 hospitals. Don Koenig, vice president of corporate responsibility for CHP, says that the first couple years after HIPAA took effect, he affirmatively asked member hospitals whether they received patients' requests for accounting of disclosures, and they said "no." He hasn't asked lately, but he assumes he would hear, and there has been no word.

Similarly, Twin County Regional Healthcare in Galax, Va., also has never had a request from a patient for an accounting of disclosures, according to corporate compliance and privacy officer Michele Bobbitt. The system is prepared if one comes in, but no investment was made in a fancy process. She would gather relevant disclosures from paper records (e.g., cancer registries)

HHS's Semiannual Regulatory Agenda Includes HIPAA Actions

HHS's Semiannual Regulatory Agenda, which features all rulemaking actions under development or review, was published in the Federal Register *on Dec. 11. Below are some actions involving HIPAA. View the entire agenda at AIS's Government Resources at the Compliance Channel at www.AISHealth.com; click on "2006* Federal Register."

◆ **In June 2007, HHS will release a proposed rule that would streamline the adoption of electronic-transactions and code-set standards.** The rule would also provide some technical corrections and clarifications to the regulations. (Sequence number 1127 in the agenda.)

◆ **HHS plans to release a proposed rule in March 2007 that would revise some of the adopted transaction and code-set standards.** (Sequence number 1129.)

◆ **This month, HHS will publish a follow-up notice to the National Provider Identifier (NPI) rule.** This notice will describe the data that will be available through the National Plan and Provider Enumeration System. It will also describe the data dissemination strategy, processes and any applicable charges for the data, according to the agenda. This notice will include a comment period. (Sequence number 1130.)

◆ **A rule finalizing the standard for electronic claims attachments will be released in September 2008, according to the agenda.** (Sequence number 1182.)

and also dispatch a medical records staffer to search the electronic medical records as well.

Contact Ruelas at fruelas@iasishealthcare.com, Foster at candace_Foster@deaconess.com, Bobbitt at mbobbitt@tcrh.org. and Hofman at jhofman@scmc.org. ✧

Regence Drills Down on Identity Theft Awareness With Members

To ensure that its members do not experience financial harm or damage to their medical records, one health plan is training them to be vigilant about reporting lost or stolen insurance cards, comparing such events to having a credit card stolen.

The Regence Group of Blue Cross and Blue Shield plans, the largest insurer in the northwest and mountain states, has devised a program with its special investigative unit (SIU) to inform the public about the dangers of lost or stolen member cards. Once reports of stolen cards and possible fraud come in, the SIU tracks charges to the cards and will also get the ball rolling with law enforcement officials, according to Alex Johnson, head of the Regence SIU and a former fraud investigator for the FBI.

"When your wallet gets stolen, you call in your credit cards right away. But what about your health plan card?" asks a statement on consumer tips released by Regence. "The latest twist on identity theft is using stolen health plan cards to get medical care or prescription drugs on somebody else's tab," it says.

The health plan member is the "first line of defense" with lost or stolen insurance cards, which contain their name and a unique member number, says Johnson. "When we dealt with the typical stolen ID in the past, we dealt with financial harm, but…having your medical records altered [if a thief uses your card] could affect future treatment, and it could take several years to have your record expunged," Johnson says. You know that someone else has used your ID, but the medical record now contains someone else's information, and providers may not let you see it, he explains.

Johnson says Regence decided to take action because of the "significant increase in identity theft everywhere." The company's SIU was getting a lot of calls about lost or stolen cards and "more aggravated cases" in different regions where IDs were stolen for medical purposes, especially for obtaining prescription drugs, Johnson tells *RPP*.

The company is now better able to track lost or stolen IDs with the program, which was put into effect in September. Here's how it works:

(1) Members have been instructed to contact Regence once they determine that the ID has been lost or stolen. A customer service representative typically takes the call, Johnson says.

(2) The customer service employee enters the information into the Regence computer system. The Regence representative documents the information from the member into an SIU complaint form on the company's intranet, Johnson explains.

(3) The SIU automatically receives that information. The SIU will then send a letter to the member advising him or her of the risks associated with identity theft, and to report the incident to local law enforcement if the ID was stolen. Another step might be to interview the member if it is determined that the ID was stolen.

(4) The company's pharmacy services department is notified since most fraudulent activity involves attempts to obtain prescription drugs. If the company determines that a new ID number is needed, the membership accounting department also is notified. In the meantime, pharmacy services will "flag" the account and monitor it for unusual activity, Johnson says. If unusual activity occurs, the department will notify the member.

(5) The customer is issued a new card and/or a new ID number.

The member is encouraged to check his or her claims data at myregence.com for any possible fraudulent claims, Johnson says. But he adds that if health plans don't give members online access to claims information, members should be checking their explanation of benefits. "A lot of people don't even look at them. But I think that with the increase of ID theft, they need to be more cognizant of what's going on," he says. "If they get a statement and they haven't had any medical services, that would be one clue [that their card is being used]," he explains.

SIUs Work With Law Enforcement

Regence has plans in Idaho, Oregon, Utah and Washington, and each plan has its own SIU, Johnson explains. The respective SIUs meet with law enforcement officials in their states to share or refer cases on a bimonthly or quarterly basis. "Once we make a referral over to the agency, they take it from there, build up a case and present it to the prosecutor," he says.

Because the program is so new, Johnson says there isn't a lot of data on how it is working, but there is a "good indication that more people are aware of identity theft," and that it's not just about their credit cards anymore. "The majority falls into the lost category," and about 20% are purse snatchings, he says.

According to Johnson, most insurance companies have an SIU or something like it and the ability to set up a program for identity theft.

He adds that some responsibility lies with providers. "If a perpetrator goes to the hospital and presents an ID card, they need to be sure that it is the member. If that perpetrator runs up bills through a stolen ID and we pay that money out, we would be asking for those overpayments back," he explains. "If providers and facilities would put a policy in place that it is mandatory to provide a picture ID, it would stop the vast majority of medical identity theft," he says.

Contact Johnson through Samantha Meese at sxmeese@regence.com. ✧

Survey Shows Interest in PHRs, Equal Worries About Theft, Misuse

Increasing numbers of Americans support personal health record (PHRs), but there's a big catch — they are also extremely worried about misuse of their data, and are calling on the government to protect them.

Perhaps the privacy and security rules have escaped their attention?

Sixty-five percent of 1,000 Americans surveyed in November said they were interested in accessing their medical records online. That percentage rose to 72% among people over age 40, but dropped to 53% for those older than 60.

The nationwide phone survey was released at the Markle Foundation conference, Connecting Americans to Their Health Care: Empowered Consumers, Personal Health Records and Emerging Technologies, which was held in Washington, D.C., last month.

According to the findings, 68% view PHRs as "a way to gain more control over their own health care and become more engaged." Twenty-seven percent felt they currently had too little control. More than 90% said "tracking their symptoms or changes in health over a secure online health information network would be very important."

They are also willing to share information, provided it is deidentified and they have "some control." Those surveyed said acceptable uses include disease outbreak detection (73%), to prevent or deal with bioterrorist attacks (58%), for quality-of-care research (72%) and to detect medical fraud (71%).

Fears Persist Despite Privacy Rule

Yet, as much as they seen benefits, Americans are also alert to risks. Eighty percent were concerned about identify theft, and 56% worried that employers would inappropriately access their records.

The survey also revealed concerns that should have been addressed by the privacy rule. For example, 77% fear their data will fall into the hands of marketers, or of employers (56%).

Exact percentages were not provided, but the survey says a majority believe "the government has a role in establishing rules and protections regarding the use of electronic health information," including rules governing the "privacy and confidentiality of online health information."

Interestingly, two-thirds said the government has a role in "setting rules to control the secondary use of information," an issue that was supposed to already be addressed through the use of business-associate and data-sharing agreements.

Can You Make a 'Safe' PHR?

If you build a better mousetrap, the world will beat a path to your door, the saying goes.

What if you built a better PHR? Could your hospital attract patients? Could your medical group gain business? Could your health plan grow your membership?

Judging from surveys like Markle's, the answer is a qualified "yes." The challenge for you, then, is to give the patients the access they want and implement controls that ease consumers' minds about privacy and security, while protecting your network itself from intrusion.

RPP asked Bob Gellman, a privacy and information policy consultant and former Congressional staff member who still frequently testifies before government panels, what sort of protections would be best. He offers the following issues to chew on.

◆ ***What are the applicable laws?*** This might be less relevant than you think. Depending on how a PHR is established and who is running it, the PHRs may be outside the scope of HIPAA and any other laws intended to protect privacy, Gellman says.

He suggests the nation might need a new class of privacy rules because "HIPAA is designed for health records run by providers and insurers," and does not, he contends, offer adequate controls and notifications to patients. So, one way to make your PHR attractive would be to offer more features than are required by current laws so that patients will have an added level of assurance.

◆ ***Who's paying?*** This is an area that is fraught with trouble and possible conflicts of interest, Gellman says. "Patients may or may not want to pay for a PHR. But if a commercial company is sponsoring and paying for the PHR, then the sponsor must be benefiting from it," he says. "If the PHR is advertising-supported, then patient records will be open to marketers, something that patients universally oppose. If an employer is sponsoring the PHR, an employee should ask why. An employer's interest in reducing health care expenditures may be at

odds with a patient's interest in obtaining adequate health care."

◆ ***Who would get access?*** "Patients, providers, and insurers have different interests that overlap sometimes and diverge sometimes," Gellman says. Design your system to keep out employers and health care providers other than those who are actively involved in patients' care, he says. Don't forget to address who the PHR is actually for. You'll need a policy that governs whether a family gets its own, whether individuals have their own, and how you would address minors.

Gellman believes patients should have full access to everything in the record and that the PHR should "contain a mechanism that allows the patient to seek correction or removal of information."

◆ ***What will it contain?*** Gellman believes patients will be "suspicious" if entities other than themselves contribute to the PHR — unless they can give approval. Consider whether you would prepopulate the PHR with data you already have or whether you would leave all entries up to the patient.

A related issue is how information is going to pass from providers into a PHR. "Even healthy individuals have multiple providers. If only some providers submit information to the PHR, then the PHR may be incomplete," Gellman says. "Of course, if all providers submit information to the PHR, it may have more information in it than the individual would like, for example, records of treatment for psychiatric illness, drug abuse, and sexually transmitted disease."

◆ ***How is it monitored?*** Gellman proposes the PHRs have "full audit controls." Patients should be notified about any new information added to their PHR, any modified and any disclosed to others. "Even accesses by the patient should be logged," Gellman says.

To read a summary of the survey, visit www.markle.org. Contact Gellman at bob@bobgellman.com. ✧

Lack of Enforcement Is Surprising

continued from p. 1

McAndrew replied that DOJ officials "don't investigate all of the referrals" that OCR sends to it." She added, "But the FBI offices across the country have taken on a number of these investigations — and we simply are not privy to how that all works out."

She said she thinks the 350-some complaints that OCR has referred to DOJ "are more technical in nature, given the language of the statute and what comes within DOJ's jurisdiction." McAndrew added that these cases "wouldn't register on many radar screens as a truly egregious criminal act."

This was surprising news; it was assumed possible criminal cases would reflect more severe violations of the rule. But even that was conjecture. Until recently, OCR did not reveal the number of complaints it refers to DOJ, giving these cases a kind of an allure.

DOJ Cases Are a Source of Mystery

Many in the privacy community, hungry for any shred of guidance from OCR, believed that these cases would reveal some new insights if only OCR would provide details about them.

Apparently not. McAndrew made it plain that these cases don't contain much usable data. For one thing, OCR does not review the cases before it sends them to DOJ.

"These cases are largely referred based on the complaint itself, because they do allege an activity that is serious enough to warrant DOJ to consider a criminal investigation," she said. "But that is all they are."

Committee member Mark Rothstein seemed incredulous. "You have not investigated those cases," he said. "We have not investigated those cases," McAndrew replied.

In comments to *RPP*, Rothstein, chair of NCVHS's privacy subcommittee, lamented this fact. "I would prefer that OCR took a more active interest in these cases, including reviewing the DOJ dispositions," Rothstein said. "Assuming that OCR reviewed them in advance of

referral to DOJ, one could argue that cases OCR considered potentially serious enough to refer to DOJ for possible criminal prosecution would be the most appropriate cases for possible civil penalties in the event DOJ chose not to proceed."

Yet, since there have been no penalties from either agency based on a complaint, "clearly, the policies of DOJ and OCR are not designed for vigorous enforcement of either the criminal or civil sanctions under HIPAA," he added.

Rothstein, director of the Institute for Bioethics, Health Policy and Law at the University of Louisville School of Medicine, told *RPP* he understood the process of referral and presumed that DOJ probably kicks out cases on the same basis that OCR does.

"OCR does not screen the cases before sending them to DOJ. My understanding is that if there is conduct alleged in the complaint that arguably violates the criminal provisions of HIPAA, it is sent to DOJ," he said. "I'm sure many of these cases are not pursued for the same reasons that OCR terminates its investigations, for example, lack of jurisdiction."

He speculated on another reason — DOJ and OCR don't agree on whether people can be prosecuted under HIPAA. "DOJ's policy that individuals may not be prosecuted under HIPAA because they are not covered entities also probably results in many dismissals of complaints," he said.

McAndrew defended OCR, saying that just because OCR has not imposed any penalties, that doesn't mean

STATE PRIVACY BRIEFS

◆ **Michigan Gov. Jennifer Granholm (D) signed a law that will tighten access to medical records and place restrictions on their disposal,** her office said on Dec. 22. Granholm has been calling for such legislation since 2002 and says it will increase patient confidentiality. The law, Senate Bill 465, requires that records be maintained for a minimum of seven years, and it provides a system for disposing of older records. It also requires facilities to notify patients when they go out of business and begin transferring or destroying medical records. The law imposes fines of up to $10,000 for failure to comply. In addition, Granholm signed an amendment to the state's Freedom of Information Act (Senate Bill 468) to make it clear that protected health information, as defined by HIPAA, is exempt from disclosure. Read the bills at www.legislature.mi.gov.

◆ **The Kansas attorney general's office will continue its investigation of abortion records after the state Supreme Court denied requests from two clinics to appoint a special prosecutor,** the office said Nov. 30. The two clinics — Women's Health Care Services of Wichita and Planned Parenthood of Overland Park — asked the court to intervene in November after current Attorney General Phill Kline (R) appeared on The O'Reilly Factor television program and parts of the records were read on the air by the host (patient identities were not mentioned). "It was alarming to us that instead of stopping him and asking how he got those records, [the attorney general] just sat there and listened," Laura Shaneyfelt, an attorney representing one of the clinics, tells *RPP*. The clinics filed motions with the Supreme Court in an attempt to protect the patients' privacy and to look into how the information was able to be discussed on the air, Shaneyfelt says. Kline's office says patient privacy is not at risk and points out that he is also looking at live birth records and DNA samples. The possible crimes he is looking at include child rape, failure to report suspicion of child sex abuse, incest and violations of the state's late-term abortion laws *(RPP 3/1/05, p. 12)*. Visit www.accesskansas.org.

◆ **Indiana Attorney General Steve Carter (R) returned all patient records that he requested from Planned Parenthood clinics in March 2005 and has dropped the demand for more records,** Planned Parenthood of Indiana said Nov. 30. A state appeals court ruled in September that patients have a constitutional right to medical privacy, and that there was no evidence that the clinics were failing to report suspected abuse — the attorney general's reason for requesting the records. The attorney general first asked the clinics for information on eight patients, which the clinics provided. Investigators then "demanded" the information of 73 patients, but Planned Parenthood refused and filed the lawsuit, the organization says *(RPP 5/1/05, p. 12)*. "The state simply did not have any legitimate reasons to burden the important privacy interests of Planned Parenthood and its patients," an attorney representing the organization said in a statement. Visit www.ppin.org.

enforcement has been lax — a sentiment OCR has repeatedly expressed.

"From our perspective, that is not a measure of the vigor with which we investigate cases or achieve enforcement activities, McAndrew said. "Many of the actions that we have achieved through voluntary compliance...we consider to be active enforcement of the rule, and we are quite proud of our record in terms of getting things fixed for individuals as well as for others systemwide."

She added that OCR doesn't entirely dispense with the rejected DOJ cases.

OCR will "take that case back" and determine "whether there are aspects of that case that are within our civil jurisdiction, and we do try to investigate those cases so that they…[are] not something that simply falls through the cracks," McAndrew said.

At the meeting, Rothstein and several other NCVHS members agreed to meet with McAndrew some time in the next two months "to take a closer look" at the DOJ-referred cases to see what can be learned.

New OCR Data Are Released

NCVHS members routinely push McAndrew to provide some information stemming from the complaints that might provide guidance for privacy officials.

McAndrew generally just gives a basic report on complaints, and the November meeting was no exception. She gave the following data:

As of Oct. 31, 2006, OCR had received 23,268 complaints, and "closed" 76% of them without action. Of the remaining 24%, OCR "obtained change or action" in 68%, and found no violation in the remaining 32%. The most common form of OCR intervention was technical assistance.

As with previous reports, McAndrew listed the top five reasons for complaints:

- ***Impermissible uses/disclosures of PHI,***
- ***Lack of adequate safeguards to protect PHI,***
- ***Refusal or failure to provide individuals with access to or copy of records,***
- ***Disclosing more than the minimum information necessary to satisfy a particular request for information, and***
- ***Failure to obtain a valid authorization for a disclosure that requires one.***

She also listed the most common entities complained against, which were private health care practices; general hospitals; outpatient facilities; group health plans and insurance firms; and pharmacies.

OCR to Tackle 'Dumpster' Cases

Pharmacies involved in so-called "dumpster cases" have actually consumed a fair amount of OCR attention, McAndrew said. In November, an Indianapolis television station reported it had found protected health information on medicine bottles and records in dumpsters in more than dozen cities (see brief, p. 12). The station brought the dumping to the attention of OCR and state authorities.

"Curiously, one of our very first complaints that we got back in April `03 was a dumpster case, and they have just continued to crop up from time to time," McAndrew said. "This is something that is really easy to stop, and we are hoping to get people to focus a little bit of attention to stop these kinds of activities. There is no reason for it."

continued

McAndrew said OCR was "giving some attention, and would continue to give some attention in the coming months to getting some wider spread corrective action attention to record abandonment."

And she promised other help was on the way from OCR.

"There are a variety of things we are looking into," McAndrew said, including "using the case information to establish more of a best practice kind of information" tool.

She said posting this kind of information on OCR's Web site is something the agency is "actively looking into." OCR could "have prominent cases posted and have resolutions put up there as well, where we think [corrective actions] have been particularly effective."

In this way, OCR would be "getting the word out," while providing examples of "things to look for in your own situation to try and prevent" infractions. For entities that have faced similar situations, the information about such incidents would reveal the "ways that other people have sought to fix them."

"These are all good uses of complaint information," McAndrew told the subcommittee, "and they're all being discussed in terms of things that OCR can implement in the future." She did not provide any timeline for completion of these efforts.

PATIENT PRIVACY COURT CASES

This monthly column is written by Ramy Fayed of the Washington, D.C., office of Sonnenschein, Nath & Rosenthal LLP. It is designed to provide RPP *readers with a sampling of the types of patient privacy cases that courts are now hearing. It is not intended to be a comprehensive monthly survey of all patient privacy court actions. Contact Ramy Fayed at (202) 861-1383 or rfayed@sonnenschein.com.*

◆ **A New York Appeals Court found that physician-patient privilege was not violated when police obtained information from a hospital administrator that identified the defendant's injury and its location.** The defendant allegedly got into a fight during which his face was cut from the left ear to his chin. The defendant was treated at Lincoln Hospital for his wound, which was stitched and bandaged. The fight provided the impetus for a subsequent shooting that led to the death of Anthony Berrios.

While investigating the homicide of Anthony Berrios, a police detective went to Lincoln Hospital and asked an administrator "if there was any male blacks that were treated on October 13 for any kind of slash wounds to the face" or "if anyone came in for a slashing to the face on that date, October 13th." The hospital administrator gave the detective an admission slip with defendant's name and address, and told him that the defendant had received stitches on the left side of his face. The defendant argued that the information provided by the Lincoln Hospital administrator as to the treatment of a person for a facial wound was obtained in violation of defendant's physician-patient privilege under New York law and his right to privacy under the Fourth Amendment. As a result, he argued that the information obtained from the violation, which led to his arrest and identification from a photo array and in a lineup, implicated a constitutionally protected right and must be suppressed from his trial.

In rejecting the defendant's claim, the court explained that the "physician-patient privilege, which generally does not extend to information obtained outside the realm of medical diagnosis and treatment," "is limited to information acquired by the medical professional through the application of professional skill or knowledge, and seeks to protect confidential communications, not the mere facts and incidents of a person's medical history." The court also did not accept the defendant's assertion that the information was privileged because it revealed the cause of his facial wound, a slashing, and that it was acquired "through the application of professional [medical] skill or knowledge." Rather, the court concluded that the information disclosed revealed no more than what had been readily observable, no medical determination was required to frame a response to police inquiry, and the information disclosed did not relate to confidential communications and thus, no violation of the physician-patient privilege existed. In reaching that conclusion, the court noted that the "[d]efendant's facial wound, a fresh scar that extended from below his ear almost to his chin, was conspicuous to the average layperson. There was no medical skill or knowledge behind the ascertainment of that information [and as such,] the hospital administrator's identification of defendant's injury and its location, and that he had received facial stitches, revealed no more than what had been readily observable."

continued

"At public sessions, covered entities have complained to OCR that the lack of enforcement translates into lower effort at HIPAA compliance," said Peter Swire, a law professor at the Ohio State University and former chief counselor for privacy in the Office of Management and Budget under the Clinton administration.

"With over 1 million covered entities, there needs to be a clearer signal that HIPAA is being enforced," he asserted.

"The lack of coordination between HHS and DOJ gives one more reason why the new Congress should look into the HIPAA enforcement system," Swire said.

"The HHS approach is to work with violators rather than ever bring a complaint. The new testimony indicates that DOJ makes HIPAA enforcement a very low priority. The new Congress should investigate what it will take to create reasonable enforcement," he added.

"The lack of coordination on HIPAA enforcement is something the two agencies should be able to work out between themselves. If there is some legal impediment to coordination, they should tell Congress what that is and get it fixed," Swire said.

Jeff Kerber, who is the manager of general consulting services at Inteck Inc., a firm that specializes in information systems at health care organizations, said "on the one hand, it is hard to imagine the two agencies are not working together to coordinate enforcement. On the other hand, we are talking about the federal government."

"The lack of communication can do nothing but continue to make the HIPAA privacy and security rules look like a farce," Kerber asserted. "The media reports cases of PHI being discovered blowing across the yards of patients, but cases like this are closed without providing OCR with an explanation. It appears that the only thing HIPAA has done is to bring patient privacy into the media limelight," said Kerber. "The lack of real enforcement and poor communication between the agencies charged with enforcing the law will allow covered entities to continue with the *status quo*," he added.

For further information, contact Rothstein at Mark.Rothstein@Louisville.edu, Swire at peter@peterswire.net and Kerber at jkerber3501@kerber-family.net.

PATIENT PRIVACY COURT CASES, continued

Moreover, the court further held that even if it were to find a violation of the physician-patient privilege, suppression of the information imparted would not be required. A violation of a statute may be remedied by suppression only if the purpose of the statute is to give effect to a constitutional right. The court found nothing in the "three vital policy objectives underlying the codification of the [physician-patient] privilege … indicating a legislative intent to confer a constitutionally derived 'substantial right,' such that the violation of statute, without more, would justify excluding such information" from defendant's trial under the Fourth Amendment. The court acknowledged that while, in certain circumstances, federal courts have found confidential medical information to be entitled to constitutional privacy protection, none of those cases held that the admission of evidence obtained in violation of the physician-patient privilege was constitutionally impermissible under the Fourth Amendment. ***(People of the State of New York v. Greene)***

◆ **The Fifth Circuit Court of Appeals held that there is no private right of action under HIPAA.** Margaret Acara filed suit against Dr. Bradley Banks alleging that Dr. Banks violated HIPAA by disclosing her medical information during a deposition without her consent. In reviewing her claim, the Fifth Circuit found that HIPAA has no express provision creating a private cause of action, nor is it implied within the statute. Supporting its position, the Fifth Circuit noted that "HIPAA does not contain any express language conferring privacy rights upon a specific class of individuals. Instead, it focuses on regulating persons that have access to individually identifiable medical information and who conduct certain electronic health care transactions." In addition, HIPAA limits enforcement of the statute to the secretary of Health and Human Services. As such, the Fifth Circuit concluded that because HIPAA specifically delegates enforcement, there is a strong indication that Congress intended to preclude private enforcement. Finally, in acknowledging that it was the first Circuit Court of Appeals to consider the issue, the Fifth Circuit noted that it was "not alone in [its] conclusion that Congress did not intend for private enforcement of HIPAA [and that] every district court that has considered this issue is in agreement that the statute does not support a private right of action." ***(Acara v. Banks)***

PRIVACY BRIEFS

◆ **Bipartisan federal support and intense private-sector interest could help with the creation of a national network of electronic health records (EHRs) in coming years, but privacy will be an issue at the forefront of the debate,** says an issue brief released in December by the Alliance for Health Reform. Other issues will include structure and financing, the brief says. The Alliance, which is a nonpartisan, nonprofit group that educates about health care issues, also says that providers have been slow to adopt EHR technology. A review of surveys conducted by the Robert Wood Johnson Foundation in 2006 found that 13% to 16% of solo practitioners have adopted EHRs, and 19% to 57% of large physician groups have adopted the technology. The brief noted that the rates "varied significantly" and added that "even assuming the higher estimates are true…IT adoption by hospitals and physicians still has a long way to go." Read the brief at www.allhealth.org.

◆ **Three major pharmacy chains have changed their policies on the disposal of patient information after an investigative report by WTHR Channel 13 in Indianapolis turned up records in "unsecured dumpsters,"** according to the station's Web site. During a six-month investigation covering several major cities, the station found more than 2,000 patient records in dumpsters at CVS, Walgreens and Rite Aid locations. All of the companies responded to the report, saying that they have reiterated their trash policies to employees and that they are taking steps to strengthen those policies. For example, Walgreens requires (1) patient vials to be disposed of at its warehouses; (2) staff members to either black out PHI or remove a label from a vial before throwing it away; and (3) outdoor dumpsters to be locked at all times. Visit www.wthr.com.

◆ **Providers, health plans and other organizations have not completed certain "key activities" and may not be in compliance before the National Provider Identifier (NPI) is implemented in May 2007,** according to a Nov. 29 letter to HHS from the National Committee on Vital and Health Statistics (NCVHS). NCVHS has been tracking implementation of the NPI and has heard testimony on the preparedness of providers, health plans, clearinghouses and software vendors, the letter says. About 1.4 million NPIs have been issued to providers, but few of those providers have communicated their NPIs to the health plans, or to the facilities where they practice. Also, few are sending NPIs in HIPAA transactions, NCVHS says. Read the letter at www.ncvhs.hhs.gov.

◆ **Concentra Preferred Systems (CPS), an Illinois-based technology vendor for some major health care payers, said on Dec. 1 that a lockbox containing backup data tapes was stolen in October from one of its satellite offices.** The tapes contained individual member benefit plan information of "several" of the company's clients, CPS said. "Based on the nature of the crime…, law enforcement authorities believe this to be the act of common thieves looking for cash or pawnable items of value, and not the act of sophisticated criminals targeting specific data," the company said in a statement. Aetna, Inc. is one of CPS's clients and the insurer estimated that the tapes contained names and either Social Security numbers or member numbers for about 130,000 Aetna, members. "Aetna believes the likelihood of anyone successfully accessing or compromising the data to be low," a statement on Aetna's Web site says. Another CPS client, WellPoint, Inc., is still working to determine the number of members impacted by the theft, says spokesman Jim Kappel. "Because the information that we provided the vendor was limited to the information that was absolutely necessary for their work, we believe the information relating to our customers is limited," Kappel tells *RPP*. The data will be difficult to retrieve because the technology needed is not easily obtained, he adds. Visit www.concentranetworks.com.

◆ **Cincinnati-based Electronic Registry Systems, Inc. (ERS), a company that manages data of cancer patient registries, says one of its computers was stolen on Nov. 23.** The computer contained information from five hospitals, including Geisinger Health System in Pennsylvania and Williamson Medical Center in Tennessee. ERS says it will withhold the names of the other hospitals until the facilities have been able to notify their patients of the incident. "Following our rigorous data protection procedures, multiple layers of security helped to safeguard the data," ERS says. "Law enforcement officials have no evidence that the theft was motivated by the intent to steal data," it adds. Contact ERS at (513) 771-7330.

If You Don't Already Subscribe to the Newsletter, Here Are Three Easy Ways to Sign Up:

(1) Call us at **800-521-4323**

(2) Fax the order form on page 2 to **202-331-9542**

(3) Visit **www.AISHealth.com** and click on "Shop at the AIS MarketPlace"

If You Are a Subscriber And Want to Routinely Forward this E-mail Edition to Others in Your Organization:

Call Customer Service at **800-521-4323** to discuss AIS's very reasonable rates for your on-site distribution of each issue. (Please don't forward these e-mail editions without prior authorization from AIS, since strict copyright restrictions apply.)