Report on
PATIENT PRIVACY

Volume 8, Number 5 • May 2008

Practical News and Strategies for Complying With HIPAA Rules

Contents

Recent Cases in New York, Arkansas Show Different Tools Available to Prosecutors

Two cases, one in New York and one in Arkansas, may shed some light on how federal officials decide whether to use HIPAA charges against individuals. While one case contains a HIPAA charge, the other, in which information on 50,000 patients was allegedly accessed and some of it sold, does not.

An employee of New York Presbyterian Hospital/Weill Cornell Medical Center (NYP) has been charged with accessing the personal information of thousands of people and attempting to sell some of that data to other conspirators, the U.S. Attorney's Office for the Southern District of New York said April 14. Although the victims were patients, there is no HIPAA charge mentioned in the complaint against him.

Dwight McPherson, who was an admission representative at NYP, is accused of identity theft and selling identities to the unnamed co-conspirators, court documents say. He allegedly took names, addresses, phone numbers and some Social Security numbers out of the facility's admissions computer system. NYP did its own audit and does not believe that any health-related information was included, the facility says in a prepared statement.

continued on p. 9

Hospitals Face Tricky Scenarios With Law Enforcement Requests for Patient DNA

To catch the notorious "BTK" killer, police collected the DNA of more than 1,300 men. In the end, it was the DNA of just one person — a woman, his daughter — that led to the arrest of the man and his subsequent confession.

Without her knowledge or consent, the woman's medical providers gave her DNA, collected years earlier during a gynecological screening test, to the police. Investigators then were able to make a close enough match to DNA found at crime scenes to identify the man as the killer of 10 people.

DNA is considered protected health information (PHI) under the privacy rule. Yet, as with many aspects of the privacy rule, its treatment of DNA is complicated, and interpretations are being challenged by new developments in investigative techniques, such as the use of a family member's DNA.

Eyed by some law enforcement officials as a treasure trove of DNA, hospitals and other covered entities (CEs) are increasingly finding themselves on the front lines when it comes to disclosure of their patients' DNA.

Privacy experts warn that compliance officers need to be prepared and know how to handle DNA requests from law enforcement officials, be aware of what they are permitted to release and under what circumstances, and whether patients must be notified. Others are also concerned that current protections for DNA that leaves a CE's hands are inadequate.

continued

It is important for hospitals to understand "you are not the police forces' data evidence warehouse," says Jeff Drummond, a partner in the health care section of law firm Jackson Walker in Dallas.

"We need to be careful about this," adds Sonia Suter, an associate professor of law at the George Washington University School of Law and an expert on genetic privacy issues. "There are conflicting issues here...the good of privacy and the good of law enforcement."

Killer Was Loose for Decades

Dennis Rader, a Wichita, Kan., resident now serving 175 years in prison, called himself BTK for his preferred method of ending his victims' lives: bind, torture, kill.

His crimes were committed from 1974 to 1991, but he was not arrested until February 2005; he offered a confession on the first day of his trial and was sentenced in August of that year.

It was his daughter's DNA sample that provided the final identifying link to him. His identity as the BTK killer had been strongly suggested by an e-mail he had sent that was traced back to church, where he had just been elected church council president.

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, Neal Learner; Executive Editor, James Gutman; Publisher, Richard Biehl; Marketing Director, Donna Lawton; Fulfillment Manager, Gwen Arnold; 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* ❑ $378

Bill Me ❑ $403

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

Police wanted to get Rader's DNA but did not want to tip him off, and theorized that his daughter had probably been seen at a university health clinic when she was a student.

The retrieval of Rader's daughter's DNA would have had to follow several steps, privacy experts say.

First, the health care provider, in this case a university health clinic, would have had to acknowledge that she had been a patient there and whether there was any DNA available to disclose to the police.

Drummond says the privacy rule probably allows a hospital or other CE to release this information without a subpoena or other court order.

But to actually retrieve a tissue sample would be a more difficult matter.

In this case BTK's daughter still had her privacy rights intact as she was not a crime suspect or a victim.

Privacy Rule Limits DNA Disclosure

DNA has extra protections under HIPAA because the potential for harm or misuse is so great. There is not yet a federal law prohibiting job or insurance discrimination (except in group health plans) based on genetic information, although it appears there could be one soon (see brief, p. 11).

"The police can't just walk in and say 'give me a DNA sample,'" says Drummond. "Well, they can, but the hospital doesn't have to give it to them without a proper subpoena or other court order."

"This was a highly unusual case, especially because it was the daughter's specimen that was sought," Mark Rothstein, chairman of the privacy and confidentiality subcommittee of the National Committee on Vital and Health Statistics, the leading government advisory panel on privacy issues, tells *RPP*.

How the privacy rule treats DNA "is very complicated," explains Rothstein, who is also director of the Institute for Bioethics, Health Policy and Law at the University of Louisville School of Medicine.

As described in an FAQ, the HHS Office for Civil Rights, which enforces the privacy rule, set out these circumstances for the release of PHI to law enforcement officials:

◆ ***"To comply with a court order or court-ordered warrant, a subpoena or summons issued by a judicial officer, or a grand jury subpoena***. The rule recognizes that the legal process in obtaining a court order and the secrecy of the grand jury process provides protections for the individual's private information (45 CFR 164.512(f)(1)(ii)(A)-(B)).

◆ ***To respond to an administrative request, such as an administrative subpoena or investigative demand or***

other written request from a law enforcement official. Because an administrative request may be made without judicial involvement, the rule requires all administrative requests to include or be accompanied by a written statement that the information requested is relevant and material, specific and limited in scope, and de-identified information cannot be used (45 CFR 164.512(f)(1)(ii)(C)).

◆ ***To respond to a request for PHI for purposes of identifying or locating a suspect, fugitive, material witness or missing person***; but the covered entity must limit disclosures of PHI to name and address, date and place of birth, Social Security number, ABO blood type and rh factor, type of injury, date and time of treatment, date and time of death, and a description of distinguishing physical characteristics. Other information related to the individual's DNA, dental records, body fluid or tissue typing, samples, or analysis cannot be disclosed under this provision, but may be disclosed in response to a court order, warrant, or written administrative request (45 CFR 164.512(f)(2)).

◆ ***This same limited information may be reported to law enforcement***:

(1) About a suspected perpetrator of a crime when the report is made by the victim who is a member of the covered entity's workforce (45 CFR 164.502(j)(2));

(2) To identify or apprehend an individual who has admitted participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to a victim, provided that the admission was not made in the course of or based on the individual's request for therapy, counseling, or treatment related to the propensity to commit this type of violent act (45 CFR 164.512(j)(1)(ii)(A), (j)(2)-(3)).

◆ ***To respond to a request for PHI about a victim of a crime, [when] the victim agrees***. If, because of an emergency or the person's incapacity, the individual cannot agree, the covered entity may disclose the PHI if law enforcement officials represent that the PHI is not intended to be used against the victim, is needed to determine whether another person broke the law, the investigation would be materially and adversely affected by waiting until the victim could agree, and the covered entity believes in its professional judgment that doing so is in the best interests of the individual whose information is requested (45 CFR 164.512(f)(3)).''

Disclosure Need Not Be Automatic

With regard to crime victims who may be brought to a hospital unconscious, "you don't have to wait until the person wakes up" to ask if you can retrieve DNA," Drummond says. "You are helping that person by tracking down the person who victimized them."

Case law — and some state laws — have held that some convicted criminals have reduced privacy rights. In addition, some states allow the collection of DNA without certain authorization from an arrested individual if he or she is a crime suspect and has already been arrested or is being held, Suter says.

Most states protect against the collection of an innocent person's DNA without a court order. The issue is also not clear when it is a family member's DNA that is being sought, she says.

"If there had not been a proper subpoena, grand jury summons, etc., the health clinic could not have provided the information, except in some really limited circumstances where the daughter, or person's whose PHI is surrendered, is thought to be a victim of a crime," adds Drummond. "DNA is specifically excluded from the information a covered entity can give for identification purposes, unless there is a subpoena."

Drummond also notes that releasing this information may, in fact, be optional. "The rule says this *may* be disclosed, not must," he says.

When faced with a law-enforcement request for PHI and when you are unsure of what to do, there is no harm in insisting on a court order to produce a requested specimen, Rothstein says.

"In general, my advice to a hospital would be that, in any doubtful, non-emergency case, require a warrant. The process of adjudicating the factual claim of the need for the information will protect all relevant parties," Rothstein says.

If when a subpoena has been produced, compliance need not be automatic, since there may be grounds to contest it, says Suter.

"The hospital is not going to get wind [of a court order or subpoena] in advance. Maybe after the fact they could try to quash the subpoena," she says.

continued

For example, in the Rader case, Suter says she would want to know that officials had tried "every other possible way" to get her father's DNA or other evidence before they came looking for his daughter's DNA.

Could the police instead have requested a search warrant and taken a comb or brush from the woman's house, and tested a strand of hair to match her DNA with her father's?

"The best advice that I can give is to try and make sure the [disclosure] request is specific and limited in scope. Is it relevant and material? There could be a challenge if the scope is overly broad," according to Suter. "We have to think about safeguards and limits," she adds.

Once you do comply, the patient likely will never know — at least from the CE. "If they have a subpoena issued by a judicial officer, there is not a notice requirement" to the patient, Suter says.

CE, Patient Can't Protect Sample

Suter says what worries her most is what happens to a sample once it has left a CE. The patient, unaware, cannot ensure it is protected, and neither can the CE itself. This could present a tricky legal challenge if the patient felt he or she had come to some harm as a result of the DNA sample being disclosed.

Given that it was obtained by the CE with the patient's understanding that it would be protected, would the CE have any liability? This is unclear today.

There is a growing push to ensure that once PHI leaves a CE and undergoes a "secondary use," it retains the same stringent requirements that HIPAA imposes. Rothstein's committee made the case that it should, in a letter to HHS sent at the end of last year. But at least for now there is no such requirement.

"What is most troubling to me is that there may not be sufficient safeguards once the DNA is collected. What happens to the samples? Are they retained — formally or informally? What are the protections," Suter asks.

Under some state laws, "an innocent individual has a right to have the sample expunged, but the onus is on the individual to request that," she says. "I think it should be on law enforcement."

Some would argue that PHI can be deidentified to provide protection to individuals, but Suter takes no comfort in that argument when it comes to DNA.

"It would be nearly impossible to completely deidentify genetic data once you have used it to identify someone," she says.

Contact Suter at ssuter@law.gwu.edu and Drummond at jdrummond@jw.com. ✧

What Should a Hospital Do When a Patient May Have Violated Parole?

If Ron Gaasch has learned one thing in his nearly decade-long career as a compliance officer at a community hospital, it's that privacy issues aren't always black-and-white — especially when they intersect with law enforcement.

This was recently brought home to him when a doctor at his hospital called a patient's parole officer to report that the man had tested positive for the presence of illegal drugs, a probation violation.

The privacy rule states that CEs may disclose PHI to law enforcement officials when "the covered entity in good faith believes [the PHI] to be evidence of a crime that occurred on the covered entity's premises; when "consistent with applicable law and ethical standards;" and when such a disclosure is made "to a law enforcement official reasonably able to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public."

In this case, the emergency physician at Gaasch's hospital, Community Hospital of the Monterey Peninsula in Monterey, Calif., knew the patient was on parole for an illegal drug conviction. And when he tested positive for a drug, the physician decided on his own to contact the man's parole officer. The man was not seen using drugs, nor did he have any in his possession.

Sometime afterward, the man's wife called to complain, first to the hospital's administration. The vice president of medical affairs at the hospital contacted the physician, and Gaasch was notified. He phoned the wife and also spoke to the physician.

Man Disputes Drug Use

Gaasch acknowledges being "somewhat handicapped" in following up the incident because he didn't want to violate the patient's privacy by talking to his wife; the patient himself did not contact the hospital. He said the wife told him that the man had not violated his parole, disputed that he had used illegal drugs, and contended that the doctor's call has jeopardized the man's parole, although she did not say it had been revoked.

The doctor told Gaasch he had the right under the privacy rule to report the man, and he gave two reasons why: because his drug use was a crime, and because by using drugs, he was a threat to his own health and safety.

Gaasch wasn't so sure about the crime angle, but tended to agree on the danger-to-himself theory.

"My understanding is that, if we feel a patient is a threat to our staff or the public, we can notify" authorities, he says. "We can also report it if we [feel] there is a crime that was committed on the premises."

Still, he wanted to be sure the hospital had not unwittingly violated the man's privacy.

Lack of Consensus From Peers

So he did a little research and reached out to his peers. To get the advice of colleagues on whether the reporting was permissible (see story, p. 1), Gaasch posted the scenario on a compliance listserv run by The Council of Ethical Organizations.

Knowing this was a complicated issue, Gaasch wasn't too surprised to read that there was no consensus on whether the doctor should have reported the man.

Wrote one poster, "You may be able to report under the exception to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public, but I would make sure the provider documented the rationale in the record."

But others disagreed. "Unless the parolee used the drugs on your premises or was in possession on your premises, no crime was committed there," said one of the two who disagreed.

Yet a fourth was more certain that the situation did warrant a call to the man's parole officer.

"We are not a hospital, but a residential provider," this individual wrote to the listserv. "We absolutely report such things to law enforcement, citing the sections of HIPAA [pertaining to personal endangerment]. Our notice of privacy practices given to every client clearly says that we will report such things to law enforcement, to protect the health and safety of our other clients.

Does Choice of Drug Matter?

Greg Young also understands the larger issues CEs face when a patient uses illegal drugs. A former cop, he says employees in this situation face a "moral dilemma," while the institution's response must show consistency.

"From a HIPAA perspective, it is probably more important that a CE maintain the appearance that it treats all its patients' information the same than it is to turn in a drug user on probation," says Young, the privacy and security officer at Mammoth Hospital in Mammoth Lakes, Calif. "If an employee comes across information that a patient is using illegal drugs and somehow knows that patient is on probation for using illegal drugs, he or she cannot reveal the patient's medical information without the patient's consent. Obviously, that's not going to happen — getting the patient's permission."

So, in deciding how to proceed, "I would weigh the seriousness of the drug use. If the person is using marijuana, I am not too concerned. If someone is using an opiate of some sort, I might drop a dime to the probation officer and anonymously suggest that the officer require the probationer to take a random drug test . . . now! If the probation officer is doing a good job, then a test will be ordered. It is usually a condition of probation that a probationer is subject to such tests at the whim of the officer," Young says.

"A probationer usually must also submit to search and seizure, meaning any law-enforcement officer may at any time search the person for drugs. Such conditions are accepted because it is better than going to jail. It also is supposed to encourage the probationer to stay on the straight and narrow," he adds.

Training Should Follow

Gaasch ultimately decided that there was a compelling reason under the privacy rule to report the patient. But he also concluded that some follow-up training with the medical staff was necessary.

"My main message will be that HIPAA is a complex law, and that we need to be sensitive to privacy issues," he says, adding that he is considering whether to write an article for the medical staff newsletter.

"We may think we are doing the right thing to report a patient who is abusing drugs, but we could be violating their privacy. It seems kind of counterintuitive, but the rule is not black-and-white," Gaasch says.

And Gaasch's final thought to the medical staff on this issue? When in doubt — and before you make that call — give him a ring. He'll be "delighted" to talk.

Contact Gaasch at Ron.Gaasch@chomp.org and Young at young@mammothhospital.com. ✧

Case Studies In Privacy Problems And Their Optimal Solutions

The following is another in an ongoing series of articles that is being written for RPP *by health care privacy and security consultant Chris Apgar, CISSP, president of Apgar & Associates, LLC. Contact Apgar at (503) 977-9432 or capgar@apgarandassoc.com.*

First scenario: A mental health clinic that prides itself on privacy protections is located in a building with a hall around the interior of the building. Patients and family members enter the front door and cross the hall to check in with the receptionist. The receptionist cannot see who enters and leaves the front door because the reception desk located in the clinic does not have a view of the front door. During a compliance audit, I was able to walk around the interior perimeter of the clinic without being questioned as to my business.

Passing by one room, a tub with the label "Patient Charts" was located by an open door. If I had been so inclined, I could have stolen the tub with confidential patient records. Moving further along the hall, I was able

to enter therapists' offices located off the hall because the doors of most offices were not locked when therapists were not present. Patient files were stacked on the therapists' desks, and the computers were logged in to the patient confidential database with no auto-logoff functionality enabled. Again, here was an opportunity to steal confidential patient records without being noticed.

Solutions: Lock Doors, Install Screen Savers

This is not an unusual situation and there are easy, low-cost solutions that need to be implemented to protect the privacy of patients and keep unwanted individuals from accessing areas where patient PHI can be stolen or inappropriately accessed. The first solution is merely a training and policy enforcement issue. Therapists need to be instructed to lock their offices when they leave, even for a short period of time. It would then be up to the privacy officer or designee to periodically check to make sure therapists actually locked their office doors. If they did not, sanctions could and should be imposed.

The second solution (and one required by the HIPAA security rule) would be to at least require that password-protected screen savers be activated, with the screen savers set to turn on after 10 or 15 minutes of inactivity. This would prevent unauthorized individuals from accessing electronic records and would meet the security rule auto-logoff requirement.

Also, a clean-desk policy needs to be implemented. If the therapists were not in their offices, all patient charts should be locked in a file cabinet or, at the very least, stored in a desk drawer out of sight of anyone entering the office.

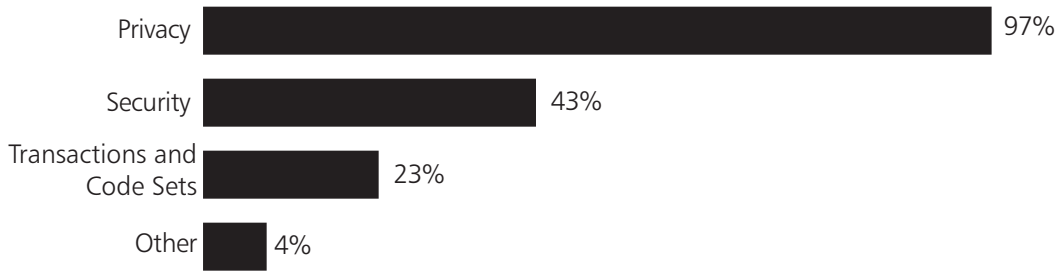
The final solution would have a small cost, but would provide the protections needed to keep unauthorized individuals from wandering around restricted areas of the clinic. The solution is to install doors at the

HCCA Survey: Compliance Officers Rate HIPAA Concerns

Hospital compliance and privacy officers' duties, goals and other job-related issues have not changed significantly from last year as compliance programs across the country mature, according to the Health Care Compliance Association's (HCCA's) annual survey. About 85% of compliance programs include privacy and information security, down from 87% last year, but those areas are still at the top of the list, the HCCA survey shows. This year, HIPAA regulation compliance is a goal in the next three years for 34% of respondents, down from 37% a year ago. The second graph below shows that compliance officer responsibility for privacy rose from 96% last year, and transactions and code sets rose from 21% to 23%, but security fell from 44% to 43%. Read more at www.hcca-info.org.

Has the Compliance Officer assumed responsibility for HIPAA compliance?

If Yes to the question above, which aspect of HIPAA is the Compliance Officer responsible for?*



*Results total more than 100% because respondents picked more than one answer.

SOURCE: Health Care Compliance Assn.'s 9th Annual Survey — 2008 Profile of Health Care Compliance Officers.

beginning of the two hallways to the left and right of the reception area, with the doors locked at all times. That would prevent anyone entering the building who is not an authorized member of the workforce from wandering back into the area where medical records are stored.

Often, privacy and related security solutions to address serious problems are inexpensive or free. This is an example where, with very little investment, serious privacy and security risks could be avoided.

Remedies Are Not Always Expensive

Second scenario: In another real-life tale, a men's HIV/AIDS clinic purchased expensive medium-security lock boxes to transport HIV/AIDS records from one facility to another. The sole reason the lock boxes were pricey was because each lock box was stamped "HIPAA Compliant." Identical lock boxes without "HIPAA Compliant" stamped on them could have been purchased from a local office supply store for significantly less money and provided the same level of security.

In this case, the clinic was following appropriate practices, but ended up spending more than they needed to because of what amounts to a meaningless stamp. In this case, the stamp could actually be viewed as adding risk. Given the stamp, someone seeing the lock boxes could then easily assume the boxes contained confidential patient information — likely something the clinic didn't want to advertise, especially given it was an HIV/AIDS clinic.

Patient Is Given Incorrect Info

Third scenario: Here is a privacy problem with a no-cost solution. I was waiting to check in at my primary care physician's office and overheard a conversation between the receptionist and a new patient. The receptionist appropriately offered the patient a copy of the clinic's notice of privacy practices and requested the patient sign an acknowledgment of receipt. The patient signed the acknowledgment and then asked what was included in the notice of privacy practices. The receptionist informed the patient that "the notice only said no information about the patient would be released to anyone without the patient's permission."

This represents a violation of the privacy rule in that the patient was not appropriately informed of the clinic's privacy practices, the patient's rights and when protected health information (PHI) about the patient could be released without the patient's consent or authorization. It was also doing the patient a disservice since he left with an understanding regarding the privacy of his PHI that wasn't true. The solution is easy and free. It is called education. All workforce members should be required to read the covered entity's notice of privacy practices, especially if they are the ones responsible for distributing the notice to patients and/or health plan members. This is part of training, and the notice should be required reading (and not just once upon hire).

Privacy and security issues arise often not because of malicious action on the part of an individual or entity. They occur because of carelessness, lack of training, insufficient assessment of risks and sometimes lack of knowledge of what is considered appropriate privacy and security practices. HIPAA aside, all health care organizations need to pay attention to potential areas of exposure of patient PHI inappropriately. Also, many of the solutions that address privacy and security risks tend not to be difficult or costly to implement. ✧

Disclosures for Public Health: Most Early Problems Have Now Subsided

Hospitals and other covered entities (CEs) appear to have overcome their initial hesitation in releasing protected health information (PHI) when reporting cases of infectious disease to public health authorities. But health privacy experts tell *RPP* that some reportable conditions may still be going underreported, and that expanded mandatory reporting could help clear up any misunderstandings.

On the other hand, some hospital officials are raising concerns about the sheer amount of patient information that must be shared with the government under new health surveillance laws.

Public health officials, meanwhile, are generally satisfied with the reporting, according to Tom Skinner, a spokesman for the Centers for Disease Control and Prevention in Atlanta. "For the most part CDC and public health official are able to go about doing their jobs when it comes to gathering and reporting public health data, while maintaining privacy issues along the way," he tells *RPP*.

HIPAA allows CEs to release PHI when reporting to public health authorities. When the law took effect in 2003, some CEs were reluctant to disclose PHI because they feared causing a privacy breach, privacy experts recall. But that situation seems to have sorted itself out, says Denise Love, executive director of the National Association of Health Data Organizations in Salt Lake City. "HIPAA doesn't seem to be as confusing to people as it used to be," she says in an interview with *RPP*.

That doesn't mean, however, that there are no potential barriers in reporting public health information. Love says that one of the issues regarding reportable diseases is that authorities may not know what they aren't getting.

"The issue may be that the individual provider or physician might not be aware that it is (a) reportable and

(b) that it is not against the law to share this information with the public health authority," she explains.

For example, if a student shows up with meningitis at a school, and the provider doesn't know the law, or doesn't know that public health authority trumps HIPAA, "they may even innocently say, 'We can't share this information with anyone,'" Love says. Physician reporting in these cases appears to be particularly low, she adds. "It may be due to privacy or…because they don't know what is reportable, or they're just not staffed properly to fully report."

The Council of State and Territorial Epidemiologists (CSTE) publishes a list of notifiable diseases each year.

CEs Say Public Health Reporting Is Routine

Hospital privacy officers say reporting to public health authorities has become routine. Megan Sopher, chief privacy officer at Truman Medical Centers in Kansas City, Mo., says she has worked for many hospitals in the Kansas City area, "none of which are reluctant to disclose the appropriate data to health officials such as the [Missouri] Health Department."

Still, Sopher asserts that moving more disease categories to mandatory reporting status would make it easier on individuals at the hospitals. "That way there, is no misinterpretation," in deciding whether something is reportable, she says.

According to Sopher, the most difficult thing to manage when reporting to public health agencies is the accounting-for-disclosures requirements, which say patients have the right to see the reasons CEs disclosed their PHI other than for treatment, payment or health care operations.

This can be an administrative burden, Sopher says. "There are so many departments within a hospital, and keeping track of all the information that is disclosed in the event that a patient requests an [accounting for disclosures] can be time consuming and complex."

Candace Foster, privacy officer at Deaconess Hospital in Evansville, Ind., agrees that the process can be burdensome in reporting public health information. But she tells *RPP* that the extent of the burden varies by hospital, and depends on members of the public's knowledge that they can request such documentation.

Overall, patient privacy regulations are not a hindrance to reporting public health, Foster says. The only concern at Deaconess, "is the ongoing need to remain current on what is statutorily reportable," she adds.

Syndromic Surveillance Requires More Data

One recent development that has caused some patient privacy concerns is Indiana's "syndromic surveillance" law, Foster says. Enacted in 2004, the law grew out of concerns about terrorism and endemic diseases, she explains. The idea is to gather "lots and lots of data from various and sundry sources" and crunch it in a computer-generated algorithm that can identify suspicious outbreaks, she says. Among other things, the law requires hospital emergency rooms to report patient information, including names, addresses and medical conditions, to the state authorities.

"You go to an emergency room, and a certain amount of data [are] just automatically going to go to the Indiana State Department of Health," says Foster. "That caused a bit of a flutter, mostly among medical records managers. There is also an element of concern over the extent to which government can intrude into the private lives of its citizens."

CEs and public agencies are able to ensure that patient information is not released, says CDC's Skinner.

"When we learn of a particular case of infectious disease, whether it's meningitis at school or tracking a case of SARS, or there is an outbreak of influenza, we're able to report information that we feel is necessary to protect the public health without giving specific information that they may jeopardize the confidentiality of the person involved," he says.

"By and large we're able to do what we need to do to protect public health when it comes to disease surveillance," Skinner adds. "And in instances where information is transmitted, there are great strides taken to protect patient confidentiality."

Contact Sopher at Megan.Sopher@tmcmed.org and Foster at Candace_Foster@deaconess.com. ✧

Cases Show HIPAA Isn't Only Remedy

continued from p. 1

Because of his job in admissions, McPherson had access to the hospital's registration system, "which is used to track patient admissions, transfers, and discharges, and contains the personal identification of patients," the complaint says. According to court documents, McPherson told investigators that he was approached by a co-conspirator and agreed to participate in a scheme to steal the records of males who were born between 1950 and 1970. He agreed to sell them to the co-conspirators, the feds contend.

The alleged scheme took place between March 2006 and February 2008, during which McPherson accessed information on 49,841 people, the feds say. McPherson sold information of about 1,000 patients for $750 at one point, according to the feds. In 2008, McPherson obtained 221 more documents that were transported to Atlanta. Agents there with the U.S. Postal Inspection Service (USPIS) had a warrant and seized them, according to the complaint.

Man Had User Name, Password for System

Investigators took the documents back to NYP employees, who explained that the system can only be accessed by those who have a user name and password. It also has a function that shows what records were accessed by which user, so NYP could see that McPherson was the user who printed the documents, the feds explain.

McPherson was "specifically trained and instructed that he may only access the…system to view records for patients that he has been specifically assigned," the complaint says.

NYP says it is contacting the affected patients. "We want to assure our patients that we take this matter very seriously and will take all necessary steps to safeguard their personal information," it says in the April 15 statement. "We have appointed an internal task force to build upon our existing systems and to develop a comprehensive program to prevent potential data theft in the future."

McPherson's attorney did not return calls seeking comment.

The U.S. attorney's office in New York refused to answer any further questions about this case, including why HIPAA charges weren't included.

Boston attorney David Szabo speculates that the feds used the obvious tools they had available to them and didn't need HIPAA for this case. "It looks like they're treating this as a fairly straightforward identity theft conspiracy" and used the Computer Fraud and Abuse Act, which states that if you exceed your authority in the use of a protected computer for financial gain, you have violated the law. "One of the things this shows, at least when it comes to computer systems, is that HIPAA is not the only remedy…. There is a whole menu of crimes to choose from," he says and adds that the feds probably could have thrown HIPAA in the criminal complaint and would have won.

Was 2005 DOJ Memo a Factor?

Szabo, who is with the Nutter, McClennen & Fish law firm, also wonders whether the feds were thinking of the June 2005 memorandum from the Department of Justice (DOJ), which said that rank-and-file employees likely would not be targeted for HIPAA criminal violations. DOJ said that only covered entities (CEs) may be directly prosecuted in such cases (*RPP 7/05, p. 1*), but it left open the possibility that individuals can be charged under an "aiding and abetting" theory. In other words, the person caused the CE to violate HIPAA, but he/she wasn't acting within the scope of his/her job.

Szabo reasons that maybe the feds didn't want to imply that NYP was at fault in the case. "This didn't require them to make any allegation that would appear to be critical of the medical center. They're saying this is clearly a guy who is off on his own…. No one would say that this was something that the hospital was trying to encourage."

All of the HIPAA criminal charges filed so far have been against individuals since the memo came out (and there was one case before it was released), and Szabo says the Arkansas example sounds like a textbook HIPAA case.

In Arkansas, Andrea Smith pleaded guilty on April 15 to wrongfully disclosing individually identifiable health information for personal gain in violation of HIPAA, according to the U.S. Attorney's Office for the Eastern District of Arkansas. She and her husband, Justin Smith, were indicted in December. Andrea Smith was a nurse at the Northeast Arkansas Clinic and took medical information for one patient and gave it to her husband, who told the patient that he would use it against him/her in an upcoming legal proceeding, the feds say (see the court case, p. 10).

The U.S. Attorney in that case vows in a prepared statement that medical employees will no longer be able to snoop for juicy details, but that HIPAA will now be vigorously enforced.

"There is a criminal provision under HIPAA that says if you are doing something with a bad motive, the penalties really escalate," Szabo says. It sounds like the feds had fewer choices in the Arkansas example, he adds, because she wasn't using the information for identity

theft, and if she took the information from the paper medical record, there was no computer involved.

So, in the New York case, could the hospital have done anything to detect McPherson's activities? "It is very difficult to immediately detect improper or excessive access by a trusted staff member," Szabo says. "[McPherson] was looking at a database that was within his job function, but he was looking at it too often and at patients he wasn't assisting."

How could a CE detect that? "They could do random audits. If they had some metrics…they could see if they need to investigate," Szabo says. "But they would have to hire a security analyst to do that, so it costs money. And in talking to privacy officers, I think a lot of systems would have to make a resource allocation decision, and it may be a tough sell to do that," he explains.

CEs could also rely on specialized security systems that flag unusual activity. But at the end of the day, "all information systems have trusted insiders. How you use either technology or auditing by humans to monitor or observe unusual activity is a challenging problem,." Szabo says.

Visit www.usdoj.gov/usao/nys and www.usdoj.gov/usao/are. Contact Szabo at dszabo@nutter.com. ✧

PATIENT PRIVACY COURT CASES

This monthly column is written by Rebecca 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 Fayed at rcfayed@sonnenschein.com.*

◆ ***A nurse pleaded guilty to violating HIPAA***. In December 2007, Andrea Smith and her husband, Justin Smith, were indicted on charges of violating HIPAA in the U.S. District Court for the Eastern District of Arkansas. Smith, a licensed practical nurse, was employed by the Northeast Arkansas Clinic (NEAC). While a NEAC employee, Smith accessed the protected health information (PHI) of a clinic patient and disclosed that information to her husband. Her husband, in turn, contacted the patient and told the patient that he intended to use the PHI in a legal proceeding. NEAC terminated Smith after she made the disclosure and was not charged in connection with this case. Recently, Smith pleaded guilty to wrongfully disclosing PHI for personal gain and malicious harm, a violation of HIPAA. For this HIPAA violation, Smith may face up to 10 years in prison and/or a fine of up to $250,000. According to the recently issued Department of Justice press release, Jane Duke, the U.S. Attorney for the Eastern District of Arkansas, stated that "[w]hat every HIPAA-covered entity needs to realize and reinforce to its employees is that the privacy provisions of HIPAA are serious and have significant consequences if they are violated. Long gone are the days when medical employees were able to snoop around office files for 'juicy' information to share outside the office. We are committed to providing real meaning to HIPAA."

◆ ***A former UCLA Medical Center employee has been indicted for selling PHI***. Lawanda Jackson was an administrative specialist at the UCLA Medical Center and was indicted in April for allegedly accessing the PHI of celebrity patients and then disclosing it to the media for commercial advantage in violation of HIPAA. She was terminated from her job on May 21, 2007. Jackson allegedly received $4,600 through checks written to her husband from a media outlet, according to court documents in the U.S. District Court for the Central District of California. The indictment was unsealed on April 29. If convicted of the charge, Jackson may be sentenced to up to 10 years in prison.

◆ ***A court found that HIPAA does not create a private right of action***. Plaintiff Olain Jones filed an action against Cariten Healthcare and The Psychology Center, alleging a violation of his medical privacy rights. According to Jones, he sought mental health treatments from Cariten Healthcare and The Psychology Center through his employee assistance program. He asked that the health care providers not contact his employer until he had received treatment. However, Jones alleges that, by contacting his employer, the defendants violated HIPAA. Citing precedent in the Fifth Circuit, the United States District Court for the Eastern District of Tennessee held that HIPAA does not create a private right of action. As the court noted, the Fifth Circuit already has held that there is no private right of action under HIPAA. Specifically, while HIPAA provides for civil and criminal penalties for violations, "HIPAA limits enforcement of the statute to the Secretary of Health and Human Services." (*Jones v. Healthcare*)

PRIVACY BRIEFS

◆ **The University of Miami (UM) said April 17 that backup tapes containing information on patients who came to its facilities since January 1999 were stolen from a storage company, but that the risk of access to the information is low**. Local media estimate that data on 2.1 million patients were affected. The university says in a prepared statement that it is contacting 47,000 people whose data may have included financial information. University officials were contacted on March 19 by the offsite storage company and told that a container carrying the tapes was stolen from a company vehicle. Law enforcement is investigating the incident as one of a series of petty thefts in Coral Gables, the UM statement says. UM says it is unlikely that thieves could access the data "because of the complex and proprietary format in which they were written." UM hired an independent company to try to extract data from a similar set of tapes, but the team was unable to do so, the statement adds. Visit www.dataincident.miami.edu.

◆ **WellPoint Inc. says it notified certain members in April that their information may have been accessible via the Internet**. *RPP*'s sister publication, *The AIS Report on Blue Cross and Blue Shield Plans* reports that the member identification numbers, Social Security numbers, and pharmacy and medical data of about 130,000 members could have been affected. A statement from WellPoint explains that data were stored on two computer servers, maintained by a third-party vendor, that were not properly secured. The insurer says it is investigating the incident, has secured the data, and is providing free credit monitoring for the affected members. Visit www.wellpoint.com.

◆ **The UCLA Medical Center is taking several steps to review and strengthen its practices on patient privacy after high-profile breaches that have taken place in recent months**, says UCLA Chancellor Gene Block in an April 10 letter to the university's president. Among the changes, UCLA has appointed a panel that will review the guidelines for access to records, and the school has engaged a consulting firm to audit its information security policies and procedures and to help define best practices, the letter says. Regarding information technology, UCLA has several plans under way, including (1) analyzing the strengths and limitations of the major clinical information systems in place; (2) expanding the auditing capabilities of such information systems; and (3) performing proactive audits for patients, based on patient requests, celebrity status, etc. UCLA Medical Center fired several employees after a breach in February in which staff members looked at Britney Spears' data (*RPP 4/08, p. 11*). The facility says one staff member resigned in May 2007 after she viewed data on about 61 people, including "recognizable celebrities and public officials." Visit www.newsroom.ucla.edu and click on "News Releases."

◆ **The President's Council of Advisors on Science and Technology (PCAST) is expected to call for changes in federal privacy laws in a future report on personalized medicine**, Government Health IT reported on April 9. PCAST will recommend that Congress amend HIPAA to protect genetic information, the Web site reports. It will also urge the American Health Information Community to "continue its work on integrating genomic information into e-health records," the article says. PCAST is appointed by the president and is made up of members from outside the government who have expertise in science and technology. Visit www.ostp.gov/cs/pcast.

◆ **The U.S. Senate passed the Genetic Information Nondiscrimination Act (GINA) on April 24 by a vote of 95-0, and the House passed it by a 414-1 vote on May 1**. "This bill will help fulfill the promise of genetic research to save lives and reduce health care costs, by establishing basic protections that encourage individuals to take advantage of genetic screening, counseling and testing, and new therapies, without fearing that this information will be misused or abused," says Sen. Mike Enzi (R-Wyo.) in a prepared statement. The law establishes protections against discrimination based on genetic information in health insurance and employment. The president is expected to sign the bill, the statement adds. Visit http://enzi.senate.gov.

◆ **A bipartisan group of senators and business leaders is encouraging the passage of the Wired for Health Care Quality Act (S. 1693)**. "Pen and paper record keeping can't keep pace with the miraculous advances being made in medical science and health care," Enzi says in a prepared statement. The bill would require privacy protections, such as notifying patients when their medical information is wrongfully disclosed. Late last year, HHS Sec. Michael Leavitt said that he was opposed to certain other aspects of the legislation (*RPP 9/07, p. 1*). The Wired Act has not been in front of the full Senate for a vote since its introduction in June 2007. Visit http://enzi.senate.gov.

PRIVACY BRIEFS

◆ **Two congressmen are investigating the theft of a laptop containing unencrypted medical information on 2,500 patients enrolled in an NIH study** (*RPP 4/08, p. 3*). The National Heart, Lung, and Blood Institute acknowledged that the lack of encryption of the data violated its policies and vowed that it is "committed to ensuring that no future security breaches will occur." Although the laptop was stolen on Feb. 23, Reps. John Dingell (D-Mich.) and Bart Stupak (D-Mich.), point out that NIH officials made no public comment about the theft and did not send letters to affected patients until March 20. "The stunning failure to act, by both NIH and HHS, raises troubling questions," Dingell said. "The committee will exercise vigorous oversight to ensure NIH and HHS protect the security of patients participating in clinical studies. We will be seeking information to determine what safeguards are in place, where the system broke down and how best to fix it." Visit http://energycommerce.house.gov.

◆ **Web-based personal health records will open doors to researchers and give them access to possibly millions of patients and data sets**, says an article by Children's Hospital Boston researchers published in the April 17 *New England Journal of Medicine*. Records that are currently controlled by hospital staff will be under patient control so they can authorize researchers to have access to lab tests, diagnoses, medications and clinical notes, the researchers point out. "While this is exciting indeed, without forethought and regulation, the tremendous benefit of PCHRs [i.e., personally controlled health records] — for research and clinically — could easily be overshadowed by problems that could arise from the unethical and uncontrolled use of patients' valuable medical information," says Kenneth Mandl, M.D., , a co-author of the article. "Who will have access to the data, for what purposes, and under what sort of regulation?" he adds. Visit www.childrenshospital.org.

◆ **Consumers have been dissatisfied with the notification process that companies use following a data breach affecting their personal information**, a Ponemon Institute study released on April 14 indicates. About 63% of respondents reported that notification letters they received did not offer direction on steps they should take to protect their information. As a result, 31% terminated their relationship with the organization. Also, 57% said they lost trust in the organization. The survey is part of the "Consumer's Report Card on Data Breach Notification" and interviewed 1,795 U.S. adults. Visit www.ponemon.org.

◆ **More than three-fourths of respondents to a Health Information and Management Systems Society (HIMSS) survey have a high level of HIPAA awareness, but only 56% say they notified patients of a security breach**. "Such high [awareness] scores are not a surprise given the HIPAA audits underway and the penalties and funding at risk for facilities found non-compliant," the survey says. "While HIPAA requires organizations to have a risk management process in place, it does not specifically identify how organizations should implement security controls. It allows them latitude to make these determinations based on risk analysis. By and large, health care organizations have not been dealing with the area of accessing data with malicious intent," it adds. The study was commissioned by Kroll Fraud Solutions and was released on April 21. Visit www.himss.org.

◆ **The Office of the Saskatchewan Information and Privacy Commissioner is investigating why dozens of boxes full of patient records were left in vacant office space in Moose Jaw**, an April 6 statement says. Six large boxes were found in the vacant office space, and officials found 73 smaller boxes in the building's basement, to which other tenants had direct access. The records are from multiple physician practices that provided services in the area, the statement says. Province officials are working to find out who last had custody of the records and therefore was responsible for them. The trustee of the records faces a $50,000 fine for individuals and $500,000 for organizations. Visit www.oipc.sk.ca.

◆ **Legislation introduced in British Columbia would give province citizens better access to their health records and strengthen privacy protections**, an April 10 statement from the Ministry of Health says. The e-Health (Personal Information Access and Protection of Privacy) Act (Bill 24) would let patients block access to their own information contained in Health Information Banks from all health care professionals unless that patient is incapacitated, the ministry says. The law also would increase fines for violations from $2,000 to $200,000. Visit www.gov.bc.ca/health.

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 the MarketPlace at **www.AISHealth.com**

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.)