Report on
PATIENT PRIVACY

Volume 7, Number 5 • May 2007

Practical News and Strategies for Complying With HIPAA Rules

Contents

Subpoena Power Is Just Routine, HHS Says, But Is There Something Between the Lines?

HHS on April 16 granted its Office for Civil Rights (OCR) the authority to issue subpoenas to ease investigations of alleged violations of the HIPAA privacy regulation. HHS says there's no great significance to this development — it's just a matter of efficiency and convenience, not a foreshadowing of big investigations to come. From now on, OCR can issue subpoenas every time it wants to obtain records or testimony from a covered entity instead of having to involve the HHS Secretary. But some HIPAA lawyers think there may be more to this development than meets the eye.

In an announcement in the *Federal Register,* HHS Sec. Michael Leavitt delegated to OCR the authority to issue subpoenas "requiring the attendance and testimony of witnesses and the production of any evidence that relates to any matter under investigation or compliance review for failure to comply with HIPAA standards and requirements related to the privacy of individually identifiable health information." If the covered entity (CE) fails to comply with the demands of the subpoena, it will be enforced in court, the announcement states. HIPAA violations are subject to civil monetary penalties.

continued on p. 10

Domestic Abuse vs. HIPAA: To Report or Not To Report After a Victim Requests Silence?

A patient presents at a hospital emergency room with injuries that she says are from falling down stairs, but the medical staff determines they are from domestic violence. She asks them not to report the incident to police. What should the staff do? Report it anyway because she could be in more danger? Or respect her wishes and protect her privacy? And how do state laws on investigating domestic abuse come into play?

This is the scenario one privacy official posed to his co-workers and to his colleagues through a listserv. "This was a good scenario that we tossed out there to see how others dealt with it," says Steve Stark, information technologies manager at Skaggs Community Health Center in Branson, Mo. "We took this all the way to our legal department ….[and] what we learned through this is that, in the state of Missouri, it is perfectly legal for a physician to report [an incident] even after a request."

With or without a victim's request, protected health information (PHI) is not protected if a crime was involved, Stark found. "Our attorney told us that if we feel that a patient is in danger, we have every right to report it [and] we could probably be held liable if we didn't."

But there is a twist. Stark says caregivers want to be cautious and not jump to conclusions or make false accusations. "You wouldn't want to do anything…that would prevent patients from seeking care because they might start to think that every time they come in, their privacy is going to be breached."

continued

Jon Burke, a consultant on privacy and security issues, agrees. He says a hospital should take advantage of all the options it has before contacting police. "If a patient comes in with a variety of wound patterns that show an abuse context, it is a no-brainer: Make the call," he tells *RPP*. But, he says, "in a normal hospital, there is a psychiatrist on call or a social worker on call. Before you put someone in the system, you really need to consider [those options]…. Try to relate to what you would do in the course of normal life. Knowing what you know, how likely would you be to report this? If you know that someone is beating the hell out of somebody else, yeah, report it. But if you're not sure, then ask."

Burke, who received Stark's scenario through a listserv, points out that "in most abuse cases, if the victim gets to the hospital, it is the spouse that abused them [who] drives them there. If the abuser knows [he is] going to jail, that victim is not going to get to the hospital."

So, to report an incident against the patient's will could put him or her more at risk, Burke says. For example, "in California, the state can take over as the plaintiff. So a guy would be out of the house that night and maybe in jail," and probably pretty upset, Burke says.

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.

In one case that illustrates confusion on this issue, a case manager at a hospital in Louisiana sued two police officers after they arrested her for obstruction of justice for delaying the investigation of a domestic abuse case. A nurse called the police to report the incident. The case manager would not let officers speak to the victim, however, saying that she had asserted her right to privacy of medical treatment under HIPAA, according to court documents. The officers allege that she barred them from seeing the victim and threatened them with a lawsuit, court documents say.

The case manager was later arrested after the officers obtained a warrant. She filed suit against the officers and the city for false arrest, seeking damages of $170,000. Part of the case manager's argument was that her actions were justified by HIPAA, according to court documents.

Josephus Verheijde, a physical therapist and bioethicist at Mayo Clinic, explains that when the nurse called police and informed them about the potential abuse, state laws went into effect, so law enforcement was under the obligation to investigate, which is "on a totally different level [than HIPAA]."

"You can ask the question, 'is any health care provider obligated to disclose this information?'" says Verheijde, who is a certified compliance professional. "[HIPAA] allows disclosure about a victim of a crime…and you can disclose if it is expressly authorized by a state or to prevent any serious harm to the victim," he points out.

Court Dismisses Case

The U.S. District Court for the Western District of Louisiana dismissed Maier's suit on March 30. Her attorney, Paul Marx, says they do not intend to appeal, but they maintain that Maier was correct. "There is no question a state cannot violate patient confidentiality provided by federal law," he tells *RPP*. "Since that issue was not before the court, anything in the ruling on that subject is just commentary, and has no legal import."

"Maier's claim that the police officers should have known that her actions were justified by HIPAA regulations and thus lacked probable cause has no basis in law or in fact," the court's opinion says. "HIPAA prohibits hospital personnel from disclosing protected health care information to third parties. It does not bar police officers from obtaining information related to a perpetrated crime directly from a patient nor does it prohibit hospital personnel from allowing police officers access to a patient who was a victim of a crime," the court explains.

Stark says this last quote from the opinion "should be added to every HIPAA training manual in existence and should be relayed to existing staff and all new staff."

"This case demonstrates the risks hospitals take on when not fully understanding the rules and regulations of HIPAA. It is the responsibility of the [privacy and security officer] to train its staff members on when and how to apply HIPAA. Case worker Maier acted as well as she knew how to at the time, but obviously was violating Louisiana state statutes…," he says.

"I think hospitals should rehearse events exactly as described in this court case and see how nurses respond," Stark continues. "Only when a nurse is presented with this type of scenario can one learn how their staff members will react…. I know it is hard letting go of PHI to anyone who is not a care provider, but ultimately we as health care professionals have a higher goal of protecting the patient and, many times, in order to accomplish this, we must rely on [law enforcement officials]," he adds.

Verheijde says it is also important to know what your state laws say. "I would think that most — if not all — states have some regulation that says these types of crimes require an investigation."

"[HIPAA] clearly…allows disclosure of information about an individual even without consent to prevent serious harm. But it's a judgment call too," Verheijde says, according to Sec. 164.512 of the HIPAA Privacy Rule.

"It is important that institutions have policies that are well written and detailed enough so the staff knows how to handle these cases. Once the call is made, you're done. The state laws take over. And most states have statutes that say [officials] will investigate domestic violence and prosecute if appropriate."

Contact Burke at (949) 874-6082, Stark at slstark@skaggs.net and Verheijde jverheijde@mayo.edu. ✧

National Review of HIPAA Compliance Finds Rampant Confusion, Mistakes

Four years after the privacy rule went into effect, hospitals and other covered entities (CEs) are struggling with basic concepts that underlie compliance, such as what the "minimum necessary" standard means. Mistrust among CEs is rampant, and many have implemented business practices in the name of privacy and security that have no basis in law.

That's one of the take-home messages from a two-year, $11.5 million study of privacy and security compliance funded by the Agency for Healthcare Research and Quality (AHRQ) under HHS.

The project, designed to show gaps that might make a national health information network difficult, also is the first large-scale look at compliance in the hinterlands. Privacy and security practices were examined in Puerto

Virginia Tech Tragedy: When Should CEs Share Information With Public?

Emergency room and other hospital personnel frequently face the issue of whether to intentionally violate a patient's right to privacy, such as when a patient they suspect is a victim of domestic violence begs for the provider to keep silent.

The case of the Virginia Tech University shooter raises similar issues. The troubled man who killed 32 and then himself last month had been hospitalized at a psychiatric hospital in 2005. He had been brought there by campus police as a precaution after he threatened to kill himself.

The man, Cho Seung-Hui, spent several nights as an inpatient before a judge ruled that although he was a danger to himself, he should undergo outpatient, rather than inpatient, treatment.

It appears that the psychiatric hospital did not notify Virginia Tech of his release or of the order for continued treatment, nor does it appear that it was under any legal obligation to do so. The hospital, of course, is a covered entity (CE) under HIPAA and, as such, has a duty to protect patient privacy.

However, does a hospital have an ethical obligation in cases such as this to make sure that campus officials monitored a patient's compliance with the treatment order?

University officials say they knew nothing about the order, or whether Cho ever received further treatment. Hospital officials have declined to comment.

Since the killings occurred, a number of issues have been raised, including whether a hospital should share information in cases like this. A secondary issue is whether institutions such as Virginia Tech should be CEs under HIPAA, a topic that is under discussion by the National Committee on Vital and Health Statistics.

It is not clear whether that would have made a difference in this case, but the hospital might have felt more compelled to share information with another CE.

What is certain is that regardless of whether Cho ever received outpatient treatment in 2005, his rampage 16 months later showed he remained very ill.

Rico and 33 states; findings were presented late last month, although a final report is due this summer.

In addition to misapplying minimum necessary to treatment, the study also documents pervasive confusion about how state laws dovetail with HIPAA, particularly in the area of substance abuse and mental health treatments, and overlapping and conflicting practices concerning patient consent policies and procedures.

These problems shouldn't be occurring, and demand attention now — regardless of any possible national health information network, said Mark Rothstein, chairman of a subcommittee that advises HHS on HIPAA. Rothstein has argued for years that HHS did not properly educate providers about the rule and that it has a virtually non-functioning enforcement system.

"Four years after the compliance date is too long to have such widespread misunderstanding," said Rothstein, chairman of the privacy subcommittee of the National Committee on Vital and Health Statistics. "The [recent] report seems to underscore the importance of comprehensive education and outreach efforts to covered entities and the public to eliminate or reduce confusion."

The project involved Puerto Rico and 33 states that together are called the Health Information Security and Privacy Collaboration (HISPC). RTI International of Research Triangle, N.C., is the prime contractor on HISPC, which is also being supported by the National Governors

RTI Report: Some Solutions to Complicated HIPAA Compliance Issues

An interim report by the Health Information Security and Privacy Collaboration (HISPC) recently released findings on covered entities (CEs') problems with the privacy and security rules and their own state privacy laws (see story, p. 1). Some solutions have also been proposed. The following information was provided by Barbara Massoudi, a senior research scientist at RTI International, the contractor on the project, during an April 26 Webcast.

◆ ***Problem: State privacy laws are old, outdated, confusing and hard to find.*** Many states have fragmented privacy laws that are scattered about their statute books; they often conflict with one another and with HIPAA. *Possible solution:* State laws need to be updated to deal with electronic exchanges; applicable laws should be collected in one place. Suggestions also include ensuring that any new legislation references old legislation and makes a specific note of whether the new legislation replaces or clarifies the old.

◆ ***Problem: Lack of trust and a concern for liability.*** The project teams found there was clearly a need to develop trust between organizations**.** A number of the states reported that concern for liability for incidental or inappropriate disclosures had caused many of the stakeholder organizations to take a more conservative approach to developing practices and policies. *Possible solutions:* The development of safe harbors and continued dialogues such as that created by this project to build trust.

◆ ***Problem: Inconsistent patient consent processes.*** State teams said that patient consent requirements often placed the responsibility and liability for appropriate release of patients' information on the provider releasing the information, and no responsibility fell to providers making the request. All states are wrestling with how to define adequate patient consent. Many states require consent, but even in those that don't, some CEs do. The project documented broad variation among the states as to what was legally required, what was appropriate for risk management purposes, what was considered a best practice, and what was feasible from an implementation perspective. *Possible solution:* a standardized form and procedure that would work nationally or on a state-by-state basis.

◆ ***Problem: Access to patient data is variable.*** The state teams cited tension between providers, hospitals and patients concerning who controls data. And a number of the providers indicated they do not think that the patients should have full access to their records, especially to the doctors' notes**.** *Possible solutions:* No details were given beyond expressing the need for standardized procedures for access.

◆ ***Problem: variations, failures related to security rule compliance issues.*** Data from the states indicate a range of problems that would appear to be related to issues addressed by the security rule. Some teams identified the lack of standard authentication and authorization protocols as a barrier to electronic health information exchange. This created mistrust between organizations and reduced their comfort levels with other organizations' standards or policies regarding who may authorize access to personal health information. There were complaints of a lack of auditing capability, poor audit programs or non-existent programs. *Possible solutions:* Standardized requirements with technical specifications may be required.

Association. On April 26, AHRQ held a Webcast with RTI to discuss findings to date and explain next steps.

The work was carried out in each state by a steering committee and workgroups. For example, a legal work group "was charged with identifying legal and regulatory drivers of those policies and whether there was a true connection between the laws and regulations and the business policies and business practices that people have followed," Loft said.

The groups reviewed real-world scenarios to determine where there were variations in privacy and security policies, so they looked at information exchanges that occurred for purposes such as treatment, payment, research and law enforcement, among others. Data were collected from a variety of CEs, including hospitals, health plans, physicians, pharmacies and others.

'Astounding' Array of Interpretations

In comparing the states last October and November, the RTI researchers found that "there was quite an astounding array of different ways of interpreting these privacy laws," John Loft, RTI's senior advisor for assessment methodology, explained at the Web conference.

"At the end of this, we had a set of business practices that were seen as barriers to health information exchange, or had no effect on it, or indeed might encourage it," Loft said. "The legal work group reviewed those barriers in order to determine whether or not there was a legal basis for the practice and, in some cases, there was not; that is, people often invented — or entities often invented — business practices and policies that had no legal basis for a variety of reasons."

But Barbara Massoudi, an RTI senior research scientist who also spoke at the Web conference, said finding such variation was not surprising. "Some of those variations were due to the flexibility that was built into the rules, and some was due to misunderstandings about how and when the rule applied," she said. "The approach that the stakeholders' organization takes in compliance becomes even more variable when you layer in the federal regulations that afford special protections for certain types of protected health information, such as health information associated with substance-abuse or mental-health treatment," Massoudi added.

The report documented pervasive confusion over the concept of minimum necessary.

"One of the issues surrounding the minimum necessary is the widespread belief that it applies to disclosures to providers for treatment purposes, even though the HIPAA privacy rule explicitly exempts this specific purpose from the minimum necessary requirement," Massoudi said. She added that when CEs do invoke minimum necessary, they do so based on their own unique definitions, and some even apply minimum necessary within their own organizations, while others do not.

CEs told RTI that complying with the standard is onerous and time consuming, and technology is no help. In fact, CEs with sophisticated EHRs are bypassing them entirely.

Some state teams reported the existing technology cannot limit disclosures to the minimum necessary, so the process that could be electronic must be manual, Massoudi said. "For organizations that use paper records, sifting through the records to make sure that the minimum necessary is exchanged is seen as time consuming and onerous, and in practice ends up resulting in variable disclosures," she said.

"So, for example, some stakeholders indicated they were required to print out copies of records from EHRs and redact especially sensitive health information or information that could not be disclosed because the EHR did not accommodate segregation of certain types of data," Massoudi said. "The current business practice is you print a paper copy, redact the information, and fax the redacted copy of the record to the intended recipient." (see box, p. 4)

For Rothstein, these problem areas as revealed by a study that did not even have this purpose means that more must be done. "The report...supports the need for an evaluation component to HIPAA," he tells *RPP*. "Systematic efforts to assess compliance issues and determine problem areas will help focus efforts on the most pressing subjects."

He also thought that the findings should prompt policymakers to abandon the idea that HIPAA is a useful foundation for a future national network. "Perhaps more than anything, the report strongly suggests that in the rollout of the nationwide health information network, it would be a mistake to put too much reliance on the existing regulatory framework of the Privacy Rule," he said. "New approaches will be needed to deal with the increased scope of health record networks and the interoperability of health records."

Possible Solutions and Next Steps

RTI's report this summer will formally specify proposed solutions to the variety of issues identified to be problems within the states. Also, most states are working on plans to keep their activities going once the formal project is over. The interim report contains a number of suggested recommendations for changes at national and state levels, including:

◆ ***A national or state-specific definition of minimum necessary, or the elimination of minimum necessary***

altogether — a proposal sure to meet with resistance from privacy advocates;

◆ ***Standardized business associate agreements because the model agreement in the rule is insufficient;***

◆ ***Standardized model consent forms that would apply to treatment and disclosures of information,*** and would clarify the difference between "consent" and "authorization;"

◆ ***A "national oversight body," a recommendation that the RTI officials did not explain,*** but which indicates the state teams do not feel the current enforcement by OCR is adequate;

◆ ***The establishment of "safe harbors" so that CEs are protected from liability for inadvertent or mistaken disclosures of PHI;*** and

◆ ***Guidance on how to comply with federal provisions on substance-abuse and mental-health records,*** HIPAA, and with state laws addressing these records.

Visit www.rti.org. ✧

Experts Expound on the Changing Environment, Role of Privacy Officer

Security breaches, state laws, complacency about HIPAA and health information exchange are just some of the concerns health privacy professionals discussed in a recent roundtable sponsored by the American Health Information Management Assn. (AHIMA)

One of the biggest concerns for privacy officers today is a security breach, says Nadia Fahim-Koster, information privacy and security director at Gwinnett Health System in Lawrenceville, Ga. **"**What keeps me up at night is having a major security breach that will bring about a privacy breach," she said at the roundtable. "We put a lot of effort into our networks and applications security, but with USB devices, camera phones, and iPods with 80 [gigabyte storage capacity], someone can download your entire hard drive and carry it away in their pocket. As fast as technology is proceeding, it's exceedingly hard to keep up. It's very disconcerting."

When asked whether there has been complacency about HIPAA from some organizations, Fahim-Koster said there is. "When we started, a lot of organizations made resources available prior to the HIPAA implementation deadline. As it came and went without complaints and no nationwide efforts by the OCR, some executives relaxed and said, 'We've done what we could do, now we need to move on,'" she says. "Privacy and security has to compete for resources that are perceived to be needed elsewhere. I hear OIG is starting its first security audits, and hopefully some guidance will come out of it…"

But John Gildersleeve, system privacy officer at Geisinger Health System in Danville, Pa., said there is not much complacency in this area. **"**I don't agree that there's complacency. The degree to which there are daily questions shows that our work-force members are taking time to ask and be very compliant with the law. There's a small percentage of the public that's aware of HIPAA or who want to exercise its rights under HIPAA, but I don't believe that leads us to be complacent. Health care has had a sense of confidentiality from day one, so certain parts of HIPAA are not new concepts; it just formalized the process for dealing with privacy and security."

Are Consumers Informed?

There was also some disagreement about whether patients are becoming more informed about health information and their rights to view it.

"People are not becoming more informed," said Joan Kiel, Ph.D., HIPAA compliance officer at Duquesne University in Pittsburgh. "They hear you can get your medical record and that yes, you can amend it, but then they hit a roadblock because they want something that's not required by the law or the hospital or physician's office misinterprets the regulations. So we as an industry need to become more informed and be more effective in explaining to the public its rights."

"Patients are receiving information, but it's not complete, nor is it being distributed by the correct people, said Jana Chvatal, manager of the privacy and information security office at Texas Children's Hospital in Houston. "Articles in consumer publications may address HIPAA but not explain the rules and/or rights correctly. Unfortunately, passage of HIPAA didn't include a means for the government to educate consumers, so they have to depend on others who might not have a complete understanding of the regulation."

When asked to comment on whether HIPAA lacked teeth for building the public's trust in privacy, Chvatal told AHIMA that HIPAA is not doing anything to reduce trust, but also is not doing anything to enforce the trust either. **"**We're not seeing OCR doing random audits, and we don't hear about them levying fines. We know some complaints have been dismissed because they weren't valid, and some may have been passed on to the Justice Department, but people are not seeing their complaints come to light, so that doesn't help them place trust in the system. And unfortunately right now they're hearing about bad things like breaches of systems and other lapses."

Gildersleeve more "teeth" were not needed at the federal level to enforce HIPAA. "It's a complaint-driven process, and that's enough to keep providers aware of their responsibilities….In a consumer-driven system, if

the consumer doesn't feel he has trust in a provider, I doubt he will use the provider," he asserted. "That applies whether the provider uses paper or electronic records. If a complaint is received, it usually results in remediation and re-education, so if everyone takes that approach, most of the concerns will go away. By the time we got new legislation with more teeth, I don't think it would be a concern any longer because organizations would have already addressed the problem."

Read the rest of the discussion at www.ahima.org. ✧

Court Says Rx Information Law Unduly Restricts Protected Speech

This article was written by Brian Gradle of the Washington D.C., office of Hogan & Hartson LLP. Contact him at bdgradle@hhlaw.com.

Concluding that the "Prescription Information Law restricts constitutionally protected speech without directly serving the state's substantial interests," a federal court ruled on April 30 that the New Hampshire law, which bars pharmacies, insurance companies and other entities from transferring or using prescriber-identifiable data for certain "commercial purposes," is an unconstitutional restriction of free speech under the First Amendment.

The U.S. District Court for the District of New Hampshire recognized that the law attempted to address important public policy concerns, such as protecting prescriber privacy, containing health care costs and promoting public health. But in applying "intermediate scrutiny" as its standard of review, the court was unpersuaded by the state's case that the law indeed promoted these interests. Regarding prescribers' privacy, for example, the court rejected the state's claim that the law promoted a "distinct interest" in protecting their privacy, and found no claim from the state that the data was used to compromise patient privacy. Instead, the court determined that the state's claim on this point was nothing more than a restatement of its contention that the law was justified as a means of protecting public health and controlling costs.

Moreover, the court found a "fundamental flaw" in the state's argument on behalf of the law: Because the state did not assert that the prescription data were being used by pharmaceutical companies and others to present false or misleading marketing messages to doctors and other prescribers, the First Amendment required the court to be "especially skeptical" of the regulation of such speech.

Finally, the court noted that the record demonstrated a number of ways in which New Hampshire could have addressed its concerns without restricting protected speech. These included limiting the providing of samples, gifts, and meals to prescribers by drug companies, to the extent the state was concerned about the promotion of improper prescribing practices. Also, the state could itself provide information to prescribers about "best practices," and develop counter-detailing programs to inform them of the cost implications of their decisions.

The case is IMS Health Incorporated, et al. v. Ayotte, No. 06-cv-280-PB, Opinion No. 2007 DNH 061 P.
Editor's Note: *As of publication, it is not known whether New Hampshire intends to appeal this decision.* ✧

PATIENT PRIVACY BREACHES

◆ **Data on almost 3 million beneficiaries of the Georgia's Medicaid and PeachCare for Kids programs are missing,** state officials said on April 9. A CD containing the data was lost while it was being shipped to a subcontractor, according to Affiliated Computer Services (ACS), a state contractor. The lost information includes names, addresses, birth dates, Social Security numbers and dates of eligibility for the programs, as well as member identification numbers for Medicaid and PeachCare (Georgia's program for children from uninsured families). "It is our assumption that has been lost or destroyed," David Shapiro, spokesman for ACS, tells *RPP*. He adds that the company is looking at its shipping policies. Contact Shapiro at (202) 393-7337. Visit http://dch.georgia.gov.

◆ **The University of Pittsburgh Medical Center (UPMC) says it is investigating how the personal information of current and former patients was posted to its Web site.** Names and Social Security numbers of 80 individuals, were posted on UPMC's radiology department's Web page. The data were part of a presentation prepared by a faculty member in 2002 that included radiological tests for some patients. "[A] copy of the former faculty member's presentation was posted on an area of the…site where faculty members share academic information with other health care professionals," the school explains in a prepared statement. "While such sharing of academic knowledge is encouraged by UPMC, the unauthorized disclosure of personal patient information in any setting or format is strictly prohibited." UPMC adds that the information was first discovered in 2005 and was taken down, but "was apparently inadvertently re-posted on the site." The school is notifying those affected. Visit www.upmc.com.

Security and Privacy Incident Response and Mitigation

This sample policy and procedure for a security incident and response team was written by Chris Apgar, president of Apgar & Assoc. LLC in Portland, Ore. Having a person or team respond to security incidents is a requirement of HIPAA security regulation. Contact Apgar at capgar@easystreet.com.

I. PURPOSE

The purpose of this policy is to define how [organization] will respond to security and privacy incidents or suspected security or privacy incidents. This includes reporting and mitigation.

II. POLICY

[Organization] will establish a privacy and security incident response team (PSIRT) to respond rapidly to any suspected security or privacy incident by identifying and controlling the suspected intrusion, reporting all findings to the [organization] security officer or designee and the [organization] privacy officer or designee and notifying users of proper procedures to preserve evidence. If a security or privacy incident does occur, it is PSIRT's role to minimize damage to or vulnerability of information resources.

III. PROCEDURE

(1) It is the responsibility of all members of [organization's] workforce to report any security or privacy incidents or suspected security incidents to the [organization] security officer or designee and the [organization] privacy officer or designee as soon as the incident is identified.

(2) The Information Services (IS) Security Department is responsible for investigating and mitigating any identified security incidents or suspected incidents. The privacy officer or designee is also responsible to assist in the investigation and mitigation if the incident involves a privacy breach. This includes investigation, mitigation and reporting findings and actions taken to the security officer or designee and/or the privacy officer or designee in a timely manner.

(3) Investigation and mitigation is the responsibility of the PSIRT.

(4) PSIRT's responsibilities include:

a. Respond to all security and/or privacy incidents or suspected incidents;

b. Convene within one hour of notification of a potential incident;

c. Identify affected critical systems, policies or practices;

d. Assess damage and scope of the incident;

e. Control and contain the breach/intrusion;

f. Collect and document all evidence relating to the incident according to established procedures;

g. Contact additional support members as necessary for investigation of a given incident;

h. Provide liaison to proper criminal and legal authorities under the direction of the security officer or designee and/or the privacy officer or designee.

(5) Security or privacy incidents can arise at any time of day and on any day of the week. Often attacks happen during non-business hours in the hope that it will go undiscovered until the damage is done. In order to react swiftly to minimize, at least one member of the PSIRT must be available 24 hours a day, seven days a week.

(6) Each core PSIRT member must be on call to respond to an incident page immediately.

(7) The SIRT will be made up of:

a. Security officer (co-team lead);

b. Privacy officer (co-team lead);

c. Other members to be defined by the security and privacy departments.

(8) All security and privacy incidents will be reported to the PSIRT member on call. The PSIRT member on call will make a quick evaluation of the information available and determine whether PSIRT activation is warranted. If so, PSIRT members will be paged.

(9) PSIRT members will report to the Data Center as soon as possible after the page is received, but required to do so within 60 minutes. If the PSIRT member is not physically able to join the team at the Data Center, he/she needs to call into the main help desk and leave a number where he/she can be conferenced in to the initial problem assessment meeting.

(10) At the time the incident is reported PSIRT members are required to:

a. Determine if the incident warrants further investigation/action;

b. Categorize the security or privacy incident;

c. Determine what, if any, outside workforce members/managers should be called (e.g., the privacy officer, legal, operations, etc.);

d. Make sure all proper procedures are followed for the investigation;

e. Make sure of the auditability of the investigation process;

f. Document the investigative steps taken and evidence gathered;

g. Provide a detailed analysis of the incident to the security officer or designee and the privacy officer or designee and, if warranted, senior management;

h. Recommend further actions/sanctions;

i. Provide liaison with appropriate law enforcement agencies as appropriate and under the direction of the security officer or designee and/or the privacy officer or designee.

(11) If outside management is called in, their responsibilities include:

a. Participate with PSIRT members in investigation and evidence gathering related to a reported incident;

b. Make recommendations to block further intrusions

(12) Security and privacy incidents will be classified as follows:

a. Class 1 incidents which require immediate PSIRT activation:

i. Attacks against a firewall;

ii. Virus attacks;

iii. Internet abuse;

iv. Attacks against a server;

v. Attacks against any system containing PHI;

vi. Inappropriate release of PHI;

vii. Loss or theft of devices or media containing PHI;

viii. Use of PHI for personal use (not related to required business activities) or gain.

b. Class 2 incidents are those referred to PSIRT after investigation within a specific department or by the help desk or other support group. Though these require PSIRT review, they may not be emergency situations and may be able to await review by PSIRT during normal business hours:

i. Suspected password misuse;

ii. Theft of property containing information assets;

iii. Request from management to review activity of a particular member of the [organization] workforce;

iv. Accidental release of PHI to an unauthorized party;

v. Fax of PHI to an incorrect number;

vi. Inappropriate access to PHI.

(13) Security and privacy incidents may be escalated depending on the nature of the incident. A class 2 incident can be raised to a Class 1 incident in the following ways:

a. The PSIRT co-team leader (the security officer or the privacy officer) determines, based on the initial investigation of a Class 2 incident, that it is more widespread or severe than previously suspected;

b. At the request of the CIO or four other director-level staff or above.

(14) All reports regarding security or privacy incidents or suspected security or privacy incidents shall be retained for six years following the conclusion of the investigation.

IV. DEFINITIONS

(1) Security Incident: A security incident is an event that threatens … information systems or has caused damage to … information system. This includes networks, applications, workstations, etc.

(2) Privacy Incident: A privacy incident is an event or action taken by a member of the workforce that exposes patient or plan member PHI to an unauthorized party or entity. It also represents use of PHI for personal use or personal gain.

(3) Privacy and Security Incident Response Team (PSIRT): Members of the workforce designated to respond to reports of a security or privacy incident or suspected security or privacy incident. They are responsible for investigation, mitigation and reporting.

(4) Workforce: Employees, volunteers, and other persons whose conduct, in the performance of work for [organization], are under the direct control of [organization], whether or not they are paid by [organization].

Subpoena Power Spurs Speculation

continued from p. 1

Subpoenas are used when OCR is having trouble getting information from a CE, an HHS official tells *RMC*. But so far, the official says, "we have dealt with many complex cases and have not needed subpoenas to this point because covered entities have been cooperative and provided information to us." (That's separate from the criminal HIPAA cases prosecuted by the Department of Justice.) However, subpoenas "are a tool we can use when needed. But we have no particular cases in mind," the HHS official says.

As for the timing of the HHS notice, "there is nothing significant about the delegation being made now," the HHS official maintains. "It was just the course of business. This delegation means if we determine we would like to use it, we have it available to us" — without having to get the Secretary to act. It streamlines the investigative authority of OCR when it can get its own subpoenas.

Lawyers Speculate About More Enforcement

As innocuous as it all sounds, lawyers speculate there may be something more between the lines of this subpoena announcement. The announcement, some lawyers say, could mean that OCR is ready to take enforcement to the next level. OCR uses a voluntary compliance approach, in which it reports an alleged incidence of noncompliance to the covered entity and a plan is worked out that will bring the CE back into compliance under OCR's watchful eye. OCR has not imposed any fines to date (that are publicly known). Lawyers wonder whether the subpoena announcement, coming out of the blue several years after the privacy rule took effect indicates that OCR is moving in a different direction.

"My gut level is that OCR will be more serious about holding people accountable under the rule," says attorney Cynthia Stamer, who is with the law firm of Glast, Phillips & Murray in Dallas. "I think they are getting their ducks in a row."

Other lawyers agree. "It could be that [the announcement] signals an intent on the part of OCR to start issuing subpoenas and becoming more aggressive, or it could be a sign they have been finding some resistance from covered entities to their authority," with CEs claiming OCR didn't have the authority to issue subpoenas directly, says Washington, D.C., attorney Brian Gradle, who is with Hogan & Hartson.

Or maybe, for the first time, OCR has "a raft of subpoenas they wanted to send but realized they had to go to the HHS Secretary, so maybe that means they want to step up enforcement activity," says Boston attorney David Szabo, who is with Nutter McClennen & Fish. "It suggests that perhaps we are moving beyond enforcement by education and consultation to a stage where we may have enforcement actions where they need to force production of documents and testimony under oath, which suggests a more adversarial enforcement process."

Some privacy officers may welcome this approach. They believe that imposing fines is necessary to lend teeth to their privacy compliance efforts. Without a government show of force, it's hard to convince their management and boards that investment in HIPAA is necessary.

But others are enthusiastic supporters of OCR's voluntary compliance efforts.

OCR Praised for Compliance Approach

"There is a tremendous lack of appreciation of the significance, and beneficial consequence, of the constructive and effective manner in which the Office for Civil Rights has endeavored to ensure compliance with the privacy rule," says McLean, Va., attorney Alan Goldberg, a law professor at George Mason University and the University of Maryland.

"When providers and other covered entities are fined, all that does is make it harder to be in compliance with the law. The money used for fines could have been used for education and compliance. So education should be primary in enforcement, and OCR has done that well." CMS has also encouraged voluntary enforcement as it tackles enforcement of the security and transaction

and data code sets rules. The complexity of the privacy rule is another reason to stick to the "encourage voluntary compliance approach," Goldberg says.

"People frequently debate and analyze and disagree about the meanings of many sentences and paragraphs and sections of the complex and lengthy privacy rule. This is not supposed to be some kind of tricky maze, with OCR saying 'gotcha' — you covered entities (and most everyone else) didn't understand something, so we will sanction you in order to teach you,'" he says. That's why encouraging voluntary compliance, which is implicitly written into the civil enforcement portion of the HIPAA statute, is so appropriate for recognition by OCR and CMS. However, OCR has also recognized that if CEs repeatedly fail to comply, "that is where consideration has to be given to a punitive remedy," Goldberg says, and therefore "covered entities should never ever take the potential for imposition of OCR civil penalties and Department of Justice criminal enforcement for granted."

Stamer says that if her clients wind up in a bind privacy rule-wise, she recommends they immediately call OCR and tell the enforcement agency that a problem has been discovered and the CE will conduct an investigation, fix the problem and get right back to OCR.

"You mitigate the problem and get on with life," she says. "If you generally try to comply, that's it, but the question is, how long will OCR let people do this? The [voluntary period] may be just about over. At a certain point, the lack of enforcement encourages lack of compliance."

Contact Stamer at cstamer@gpm-law.com, Gradle at bdgradle@hhlaw.com, Szabo at dszabo@nutter.com and Goldberg at alan@goldberglawyer.com. ✧

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 Fayed at rfayed@sonnenschein.com.*

◆ **The Supreme Court of Oklahoma held that the disclosure of PHI pursuant to a court order permitting, rather than mandating, *ex parte* communications does not violate HIPAA.** The petitioner, Margie Holmes, who represents the estate of Teresa Lee Elam in a medical malpractice case related to Elam's death, filed a motion to enjoin the respondent, trial judge Rebecca Brett Nightingale, from enforcing an order authorizing the release of PHI. Elam was injured in an automobile accident and subsequently died while under the care of Interim Healthcare of Tulsa and St. John's Health System, Inc. Following the petitioner's failure to execute HIPAA-compliant authorizations, the health care providers filed an application for release of PHI. The respondent ordered the release, which permitted the providers to "orally communicate and to discuss such 'protected health information' if they choose with the parties' attorneys of record in this action." In seeking to enjoin enforcement of the judge's order, the petitioner argued that the trial court's "order allowing *ex parte* oral communications with Elam's health care providers violates HIPAA's confidentiality requirements." Although the petitioner acknowledged that HIPAA allows the disclosure of PHI pursuant to court orders, she contended that "only an order compelling the release of protected health care information, rather than an order allowing such release, will satisfy HIPAA requirements." The court, however, disagreed, finding that HIPAA requirements were not contravened when the "court order clearly allows such disclosures" because (1) HIPAA allows the release of PHI in the course of any judicial or administrative proceeding "in response to an order of a court" and (2) the "clear language of the regulation anticipates…disclosures may be allowed where a court order so provides." The court did, however, reject the health care providers' assertion that "as long as there is an order signed by a judge, there is no limit on the scope of disclosure of protected health information…under HIPAA." The court explained that such an argument "ignores the rest of the sentence which requires the 'covered entity [to disclose] only the protected health information expressly authorized by such order," [and thus,] "clearly a limitation on the scope of permitted disclosure is imposed." "The privacy requirements of HIPAA apply whether or not there is court authorization for the disclosure of protected medical information." In also considering state law issues, the court further explained that the order should limit the disclosures to the "condition of the patient that is relevant to the claims or defenses asserted in the malpractice action" and should "clearly provide that no physician may be compelled to participate in oral *ex parte* communications." ***(Holmes v. Nightingale)***

PRIVACY BRIEFS

◆ **The Texas Attorney General's Office filed a lawsuit against CVS/pharmacy on April 17 seeking injunctive relief and civil penalties for its alleged violations of the state Identity Theft Enforcement and Protection Act.** According to court documents, "thousands" of business records with "sensitive personal information" of customers were found in a dumpster behind a CVS pharmacy in Liberty County. The store was either vacant or was being vacated, the suit says. The documents included copies of sales receipts with names, credit card numbers, expiration dates and other information. There were also several copies of prescription labels with the customer's name, birth date, address, prescription identification number, insurance company and name of medication, the suit says. "[CVS] failed to shred, erase, or otherwise make the sensitive personal information unreadable or undecipherable," the suit says. CVS says the documents in question did not involve recent transactions or prescriptions. "The disposal of this information in the store dumpster was a violation of our record retention and privacy policies. Following an internal investigation, the store manager was separated from the company and we have cooperated fully," CVS adds. To see a copy of the lawsuit, go to www.oag.state.tx.us and click on "News Releases."

◆ **HHS launched a Web site on April 20 that is dedicated to HIPAA compliance and enforcement and will "make it easier…to get information about how the department enforces health information privacy rights and standards."** The site shows privacy rule enforcement activities, the results of those activities and statistics on complaints, HHS says. It also gives information on consumers' rights to access their health information and control how their information is used and disclosed. Visit www.hhs.gov/ocr/privacy/enforcement.

◆ **CMS has posted new Frequently Asked Questions (FAQs) to help Medicare providers with their contingency plans for the National Provider Identifier (NPI).** For example, one question asks, "If a complaint is filed against me for not being in compliance with the [NPI] after May 23, 2007, what will happen?" To view the FAQs, go to www.cms.hhs.gov/NationalProvIdentStand, scroll down to "Related Links Inside CMS" and click on "NPI Frequently Asked Questions."

◆ **A bill under consideration by Maine lawmakers would curb data mining of prescription drug information, which is considered "a fundamental violation of privacy,"** said two organizations in an editorial published in the *Kennebec Journal*. "The drug industry, the private health data companies and others profiting from data mining have huge budgets to oppose this legislation," wrote the National Physicians Alliance and The Prescription Project. "They falsely claim it will prevent the use of prescribing data for education, research and to notify doctors of safety concerns. But LD 838 explicitly allows collection of data for these purposes, and there are existing non-commercial systems to address these needs….The bottom line is that protecting privacy and promoting good medical practice based on science, not marketing, would be good for doctors, the state and all of us." Visit http://npalliance.org. Read the bill at http://janus.state.me.us/legis.

◆ **Health care information technology experts said an internal security breach is their primary concern about their organizations' data security,** according to the 18th Annual Healthcare Information and Management Systems Society (HIMSS) Survey. About 18% of the respondents said they had experienced a security breach in the past six months, according to HIMSS. Also, 25% of those surveyed said that their organizations participate in a Regional Health Information Organization. HIMSS interviewed 360 individuals between Dec. 20, 2006, and March 1, 2007. Visit www.himss.org.

◆ **A computer server containing information on cancer research subjects was stolen from the University of California, San Francisco (UCSF),** the school said on April 18. UCSF said it has not yet determined the exact number of patients involved, but added that it has sent out 3,000 notification letters already. The files contained names, contact information, Social Security numbers and — for some subjects — personal health information, UCSF says. There is no indication that the information has been accessed or is being used for unauthorized purposes, but the police have been notified, the school says. Visit www.ucsf.edu.

◆ **Blue Care Network HMO, a Blue Cross Blue Shield plan in Michigan, is investigating the theft of members' data from an employee's car,** the insurer says. The data on the 262 members contained in printed reports, but did not include medical records, according to a spokesperson. The plan has informed the members and offered them free credit monitoring. The insurer says there is no indication that the data have been used illegally. Visit www.mibcn.com.

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.)