Report on
PATIENT PRIVACY

Volume 5, Number 4 • April 2005

Practical News and Strategies for Complying With HIPAA Rules

Contents

Call (800) 521-4323 to order a free 30-day trial of AIS's HIPAA Security Compliance Guide.

Managing Editor
Nina Youngstrom

Assistant Editor
BJ Taylor II

Editorial Assistant
Eve Collins

Executive Editor
James Gutman

Some Social Workers Cite Child-Abuse Reporting Problems Due to HIPAA

On paper, little has changed because of HIPAA in the arena of PHI disclosures for child-abuse reporting and investigations. The privacy rule defers to state law on these matters, which means everyone should follow the same state-mandated rules they have always followed. Also, the rule explicitly allows covered entities (CEs) to reveal PHI to the proper authorities when child abuse is suspected.

In practice, however, some child protective services workers and administrators say that HIPAA sometimes obstructs or delays child-abuse reporting and investigations, and they're advocating amendments to the privacy rule.

Depending on who you ask, HIPAA is either a scapegoat for state privacy protections that have always existed, or a new threat to children who may be victims of abuse.

"The privacy rule does not in any way shape or form alter what is current existing state law on child abuse reporting," says Chicago attorney Brian Annulis, who is with Katten Muchin Zavis Rosenman. It clearly allows disclosures for child-abuse reporting and investigations to continue uninterrupted:

◆ Sec. 164.512(a) permits CEs to comply with laws requiring PHI use and disclosure (e.g., state laws mandating child- abuse reporting) without an authorization or court order.

◆ Sec. 164.512(b) allows CEs to disclose PHI to appropriate government authorities that are designated to receive reports of child abuse or neglect.

◆ Sec. 164.512(c) does the same thing as (b), but refers specifically to reports of abuse, neglect or domestic violence. *The only big change:* When CEs disclose PHI for a child abuse report or investigation, they must log it in the accounting of disclosures.

continued on p. 8

OCR: No Fines Have Been Assessed Yet, As Voluntary Compliance Is Still Working

The HHS Office for Civil Rights (OCR) is still carrying a big stick without actually using it, resolving thousands of alleged privacy violations without levying any fines.

Covered entities (CEs) accused of violating the privacy rule continue to cooperate with OCR in achieving compliance voluntarily, so there's been no need to fine them, says OCR Director Rick Campanelli.

"It's important for us to send the message we are serious about enforcement and compliance. We are aggressively pursuing these complaints," Campanelli tells *RPP*. "Covered entities have been very responsive when we contact them with an investigation. We have been able to achieve compliance successfully."

As of Feb. 28, he says, 11,280 privacy complaints have been filed against CEs since the April 2003 effective date of the privacy rule. Of them, 63% have been resolved,

which means either a cooperative CE fixed its problems under OCR's supervision or the complaint wasn't a privacy violation, he says.

Campanelli says OCR isn't averse to fining wayward CEs if it's necessary, he says. However, the mere potential for a fine is apparently still motivating CEs to do the right thing.

CEs Are Focused on Compliance

"I think there is a sense out there that because the rule has civil and criminal penalties, that is an important incentive to comply," he says. "Covered entities are still very focused on their need to comply with the rule."

"The privacy rule encourages us to seek informal resolution and voluntary compliance. That is the most effective way to get the rule effectuated," he says. In fact, the privacy rule describes circumstances where imposing penalties will not be permitted. For example, OCR can't fine a covered entity when the failure to comply is "due to reasonable cause and not willful neglect," Campanelli 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.

Copyright © 2005 by Atlantic Information Services, Inc. All rights reserved. No part of this publication may be reproduced or transmitted by any means, electronic or mechanical, including photocopy, FAX or electronic delivery without the prior written permission of the publisher.

Report on Patient Privacy is published with the understanding that the publisher is not engaged in rendering legal, accounting or other professional services. If legal advice or other expert assistance is required, the services of a competent professional person should be sought.

Managing Editor, Nina Youngstrom; Assistant Editor, BJ Taylor II; Editorial Assistant, Eve Collins; Executive Editor, James Gutman; Publisher, Richard Biehl; Marketing Director, Donna Lawton; Circulation Manager, Kristin Mulcahy; Production Coordinator, Melissa Muko

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

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* ❑ $352

Bill Me ❑ $377

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

E-ALERTS FOR SUBSCRIBERS ONLY: E-mail alerts are rushed to *RPP* subscribers when timely news breaks. To receive this free subscriber-only service, send an e-mail to "RPPALERT@aispub.com" and say "sign me up." You'll also receive a free e-mail edition of *RPP* on the day of publication, in addition to the print copy.

However, imposing a fine may be in OCR's future. "If we can't get there, we are in a position to pursue [fines]. We haven't needed to do that yet. We want to encourage entities to voluntarily comply, but if they don't, we will avail ourselves of these other remedies."

OCR has referred more than 175 alleged privacy violations to the Department of Justice for potential criminal prosecution, he says. The Justice Department reviews the cases and "passes them to the U.S. Attorney in the jurisdiction where the alleged violation took place," a spokesman says. "If that office determines there's been a violation, it would proceed." He declined to comment on the specifics.

There has been one prosecution so far, when the U.S. attorney in Seattle prosecuted Richard Gibson, a former Seattle Cancer Care Alliance phlebotomist, who pleaded guilty in federal court to wrongful disclosure of individually identifiable health information for economic gain *(RPP, 9/04, p. 1)*. Gibson was sentenced to 16 months in prison last year in connection with his theft of a cancer patient's identity, which he used to obtain credit cards and purchase $9,000 worth of merchandise.

What Are the Most Common Complaints?

OCR is still investigating 37% of the 11,280 complaints, he says. "We have a very broad array of complaints about violations that touch on almost every area," Campanelli says. They overwhelmingly involve direct patient contact.

The top five most common types of complaints, he says, are:

(1) Impermissible disclosures (e.g., gossiping to a friend outside the hospital about the medical condition of a neighbor who is a patient);

(2) Lack of adequate safeguards (e.g., leaving files around, not protecting PHI on computer screens);

(3) Refusal or failure to provide access to — or a copy of — medical records;

(4) Disclosure of more than the minimum necessary protected health information; and

(5) Failure to include valid language in patient authorizations for PHI disclosures.

"It's very clear that direct contact is where people are observing violations," Campanelli says. "It's good for covered entities to recognize this and concentrate their preventive efforts" here.

The fifth top offense used to be failing to provide the notice of privacy practices, but compliance in this area has improved, he says.

For more information, contact OCR spokeswoman Christina Heide at Christina.heide@hhs.gov. ✧

EDITORIAL ADVISORY BOARD: ***MICHAEL D. BELL***, Esq., Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C., Wash. D.C.; ***JOHN BENTIVOGLIO***, Esq., Arnold & Porter, Wash. D.C.; ***MICHAEL DOSCHER,*** Senior Manager, Global Healthcare Div., Covansys Corp., Glendale, Calif.; ***BRIAN GRADLE***, Esq., Hogan & Hartson L.L.P., Wash., D.C.; ***REECE HIRSCH***, Esq., Sonnenschein Nath & Rosenthal L.L.P., San Francisco., CA; ***JAMES PASSEY***, MPH, Director, Compliance & Risk Management, Valley Health System, Hemet, Calif.; ***ERIC S. TOWER***, Esq., Associate General Counsel, Advocate Health Care, Oak Brook, Ill.

How to Determine Whether Universities Must Comply With HIPAA

Some confusion has evidently existed on the question of whether universities (or portions thereof) are "covered entities" for purposes of HIPAA privacy compliance. To address these questions, the following article was written for RPP *by Melissa K. Bianchi, an attorney in the Health Group at Hogan & Hartson, Washington, D.C. Contact Bianchi at MKBIANCHI@HHLAW.com*

While a university's primary mission is education, many universities are also health care providers. For example, universities may provide health care in clinics, student health centers, or as a part of faculty practice plans associated with medical or dental schools. In many cases, HIPAA privacy regulations will apply to these types of health care providers that are affiliated with a university.

Universities that provide health care must evaluate whether the requirements of the HIPAA privacy rule apply and, if so, to what extent. Typically, only limited components of a university are engaged in the delivery of health care. Thus, the regulatory scheme set forth by the privacy rule may be difficult to implement in the context of a university.

This article provides a brief overview of (a) the ways in which a university may be subject to the privacy rule, (b) how to structure a university as a hybrid entity to facilitate HIPAA compliance, and (c) the administrative safeguards a university must establish to ensure proper separation of the hybrid entity's health care component from the rest of the university.

Step 1: Is the University a 'Covered Entity'?

The first step in determining how the privacy rule applies to a university is determining whether the institution is a "covered entity" (CE). The privacy rule applies directly to three kinds of CEs: (1) health care providers that transmit health information in electronic form in connection with specified transactions, (2) health plans, and (3) health care clearinghouses. Also, the privacy rule indirectly applies to "business associates" of CEs.

Many universities are CEs under the privacy rule because one or more divisions within the university offer health care services and bill for those services electronically. A university also may act as a business associate. Finally, certain health plans sponsored by the university also will be CEs that are subject to the privacy rule *(RPP, 2/05, p. 6)*.

In determining whether a university is a CE by virtue of its role as a health care provider, the institution must consider first whether any of its divisions provide health care and, if so, whether they engage in electronic transactions. Electronic transactions often include the electronic transmission of information in connection with billing, health plan eligibility determinations, and health plan enrollment or disenrollment. (Most health care providers perform at least one electronic transaction and therefore qualify as a CE for purposes of privacy compliance.)

Once a university has identified its covered health care providers, it should determine whether they share identifiable patient information with any other departments within the university.

Student Health Centers: A Possible Exception: University student health centers, while clearly health care providers, may not engage in electronic transactions and may therefore not be CEs. For example, a student health center might not bill for services, or do so electronically. If the student health center does not perform *any* electronic transactions, it is not a CE and is not required to comply with the HIPAA privacy rule.

Even in cases in which student health centers qualify as HIPAA CEs, they are not subject to HIPAA with respect to the medical records they maintain on university students because the HIPAA definition of "protected health information" excludes records protected under the Family Educational Rights and Privacy Act (FERPA). This means that the use and disclosure of many, if not all, health records maintained by student health centers are subject to FERPA, but not to HIPAA. Thus, even where the student health center is a CE — because it is a provider engaging in electronic transactions — the individually identifiable health information held by the student health center would be exempt from the HIPAA privacy regulations.

However, the privacy rule would apply to the medical records of a student health center that are related to non-students — such as faculty, staff or family members of students. University student health centers that treat both students and non-students will need to determine which of their records are subject to HIPAA and which are subject to FERPA. They also will need to decide whether, as a general approach, to apply the more stringent HIPAA requirements to FERPA records, or to treat those types of records differently.

Step 2: What Is the Most Appropriate Structure For HIPAA Compliance?

Once a university has identified itself as a CE — because one or more of its divisions meet the definition of "covered entity" — it needs to determine the most appropriate and efficient way to facilitate privacy compliance. Many universities choose to designate themselves a "hybrid entities," a privacy rule construct that

Go to www.AISHealth.com to sign up for FREE e-mail newsletters —
Business News of the Week, Government News of the Week *and* Today in E-Health Business.

continued

allows organizations to separate out the divisions that actually provide health care and require privacy rule compliance of only those divisions. The advantage of designating the university as a hybrid entity is that privacy rule requirements would then apply only to uses and disclosures of information by the institution's "health care component," and not to other parts of the university. Universities that choose not to designate themselves as hybrid entities may find certain consequences that had not been anticipated, such as limitations on the use and disclosure of PHI that may exist in historical documents at a library associated with a university hospital or medical center.

Hybrid entities: The privacy rule permits a CE to minimize its compliance burden by designating itself as a "hybrid entity," allowing a university to carve out its HIPAA-covered activities (i.e., "health care component") from its other operations. Under the hybrid entity structure, only programs and activities within the university's "health care component" must comply with HIPAA privacy requirements. In order to be a hybrid entity, the university must designate its "health care component," which *must* include those parts of the hybrid entity that would be subject to the privacy rule if they were separate legal entities. In addition, the health care component *may* include any part of the university that (1) performs HIPAA-covered functions, including non-covered health care provider activities; or (2) provides "internal" business associate services to or for the health care component. No other activities or components of the hybrid entity may be included in the health care component.

Many universities choose to designate as part of its health care component any department that provides business associate-type services for or on behalf of the health care component. For example, a university may wish to include its general counsel's office in the health care component, as well as other non-provider departments or functions to the extent that such departments create, receive, or use health information to provide services for or on behalf of the university divisions within the health care component. The advantage of including these types of departments in the health care component is that it eliminates any need for the university to obtain patient authorization in order to disclose PHI to a unit outside the health care component. Under the privacy rule, a health care component would need to obtain an individual's authorization in order to disclose PHI to another university division for the purpose of performing services for or on behalf of the health care component. The alternative to this authorization requirement is to include the "business associate" division in the health care component.

Universities also may elect to place within the health care component those programs and departments that provide health care services but do not bill electronically for such services or otherwise conduct HIPAA-covered transactions. In making this decision, the university should take into account the need, if any, to use PHI maintained by the health care component to deliver such services. For example, in the case of a student health center that would not on its own be considered a CE, the university would not be required to include the student health center in its health care component because the student health center would not on its own qualify as a covered entity. Under the hybrid entity provisions of the privacy rule, however, if the student health center performs covered functions or provides certain services to any part of the university's health care component, the student health center would be required to comply with HIPAA. Even where inclusion in the health care component is not required, the university may choose to include the student health center in its health care component to facilitate any necessary exchange of health information between the student health center and other parts of the health care component.

Health plans: Finally, in designing a hybrid entity, it is important to keep in mind that a university's health plans that are covered entities may not be designated components of a hybrid entity and must instead be treated as separate covered entities.

Step 3: Implement Policies and Procedures For The Health Care Component.

In effect, the HIPAA privacy rule treats the health care component as a separate legal entity. Its requirements generally will apply only to uses and disclosures of information by the health care component and not to other parts of the university. The sharing of PHI within the health care component is considered a "use" of the information, while the transfer of PHI outside the health care component, even to other parts of the university, is treated as a "disclosure" of that information.

For this reason, the hybrid entity must establish administrative safeguards to ensure that its health care component does not improperly share PHI with any other part of the entity. With respect to its health care component, a university must restrict the use and disclosure of PHI by the health care component as required by the privacy rule. The health care component also must develop and distribute a notice of privacy practices and use good-faith efforts to obtain patient acknowledgment of receipt of this notice.

Policies and procedures must be developed and implemented with respect to the health care component to ensure that employees who perform functions both inside and outside the health care component do not improperly use PHI for the university's non-health care component activities. Through these policies and proce-

***Call 800-521-4323 or visit the MarketPlace at www.AISHealth.com for more information on AIS's detailed* HIPAA Patient Privacy Compliance Guide.**

dures, the health care component also must establish reasonable and appropriate safeguards to protect the confidentiality of PHI, implement procedures for responding to and complying with individual rights, and comply with administrative requirements, such as designation of a privacy officer, handling of complaints, mitigation of violations or privacy, and certain documentation requirements.

New HIPAA Enforcement Procedure Mirrors Privacy Rule Strategy

The new CMS procedure for enforcing various HIPAA administrative simplification regulations (except privacy) — published in the March 25 *Federal Register* — mirrors the privacy rule's enforcement framework. For example, "CMS will work with covered entities on voluntary compliance," according to CMS, the same way the HHS Office for Civil Rights approaches privacy violations. But it looks like there could be confusion surrounding which enforcement agency will prevail when a violation involves both the security and privacy rules.

The CMS procedures for filing complaints against covered entities (CEs) deal with violations of the Transaction and Code Set Rule (TCS), 65 FR 50313 (Aug. 17, 2000); the National Employer Identifier Number (EIN) Rule, 67 FR 38009 (May 31, 2002); the Security Rule, 68 FR 8334 (Feb. 20, 2003); the National Provider Identifier Rule, 69 FR 3434 (Jan. 23, 2004); and the National Plan Identifier Rule (currently under development).

The new enforcement measures are very similar to those for HIPAA privacy violations, says attorney Mike Bell. "CMS will take a substantially similar tack with these administrative simplification provisions as HHS has done with privacy, and it adds some clarity." For example, if CMS believes a violation occurred, it will notify the CE and then work with it to obtain compliance, just as OCR does, Bell says. "If CMS determines a compliance failure occurred, it will notify the covered entity of the alleged failure — just like OCR does with privacy — and then CMS will work with the covered entity to obtain compliance if, in fact, the complaint has merit," says Bell, who is with the law firm of Mintz Levin in Washington, D.C.

How Will This Work?

The new procedure, which takes effect April 25, isn't actually a regulation — it's just a notice, says attorney Reece Hirsch, who is with Sonnenschein Nath & Rosenthal in San Francisco. "There are no provisions that add to the security or other regulations. It just states what rules must be followed."

Complaints must (1) be filed in writing, either on paper or electronically; (2) explain the alleged violation; (3) include contact information (including name, address and telephone number for both the person complaining and the CE); (4) be filed within 180 days from when the person complaining knew (or should have known) the misconduct occurred. People filing complaints have the option of using a form on the CMS Web site at http://www.cms.hhs.gov.

When a complaint is submitted, CMS first will decide whether to process it or reject it. If it accepts the complaint, the agency will quickly check whether it's complete and appears to allege an actual violation of an administrative simplification provision. If necessary, CMS will seek more information from the complainant. The agency will inform the complainant if it accepts the complaint for further review.

CMS will close a complaint if it doesn't allege a true violation of an admin simp provision. Complainants themselves can also withdraw their complaints, but once the ball is rolling CMS has the right to pursue a complaint even if the person who filed it backs off.

After the preliminaries are completed, CMS will dig in. At any time during the investigation, CMS may ask the complainant for more information. "If based on the preliminary review and any additional information-gathering CMS ascertains that a compliance failure by a covered entity may have occurred, CMS will advise the covered entity that a complaint has been filed and will inform the covered entity of the alleged compliance failure," the notice says. In other words, the CE won't be informed of the investigation unless and until CMS confirms the violation occurred.

(continued)

More HIPAA Resources From AIS

✔ ***A Guide to Auditing and Monitoring HIPAA Privacy Compliance***, a softbound book with 214 pages of how-to guidance on effective auditing and monitoring systems; includes templates on a free CD.

✔ ***HIPAA Patient Privacy Compliance Guide*** (updated quarterly), the industry's leading compliance looseleaf service with more than 1,000 pages of how-to chapters with extensive policies, procedures and other practical tools.

✔ ***HIPAA Security Compliance Guide*** (updated quarterly with monthly newsletters), a highly practical 14-chapter looseleaf featuring clear explanations and dozens of policies and procedures for complying with the April 2005 deadline.

Visit the AIS MarketPlace at www.AISHealth.com

Copyright © 2005 by Atlantic Information Services, Inc. All rights reserved. Reproduction by any means — including photocopy, FAX or electronic delivery — is a violation of federal copyright law punishable by fines of up to $150,000 per violation.

CMS Will Help CEs Become Compliant

The next step: "CMS will work with covered entities to obtain voluntary compliance," the notice says. CMS will start by asking the CE to respond in writing to the alleged violation with one of the following: (1) a statement demonstrating compliance; or (2) a statement "setting forth with particularity" why it disagrees with the allegations; or (3) a corrective action plan. CEs have a reasonable time to write this up, usually 30 days.

When the CE disagrees with the allegations, it should "set forth and document" compliance; how the CE thinks the allegations are factually wrong or incomplete; why its alleged actions amount to a compliance failure. After CMS gets this documentation, CMS may have some more back-and-forth with the CE "and request the opportunity to interview knowledgeable persons or to review additional documents or materials."

At any time during this process, a CE can amend or supplement its response or propose a corrective action plan to achieve voluntary compliance. If the corrective action plan is accepted, CMS will actively monitor it and the CE will have to report periodically to CMS on its compliance progress.

Once compliance is achieved, CMS will inform the covered entity.

"If the covered entity fails or refuses to provide the information sought, an investigational subpoena may be issued in accordance with 45 CFR 160.504 to require the attendance and testimony of witnesses and/or the production of any other evidence sought in furtherance of the investigation," the notice states.

If voluntary compliance to correct a violation doesn't work out, HHS can pursue other options, such as civil money penalties.

OCR Issues Two New FAQs

On March 8, the HHS Office for Civil Rights (OCR) released its responses to two additional frequently asked questions (FAQs). Visit www.hhs.gov/ocr/hipaa, where these and other FAQs are archived.

(1) "May a health plan disclose protected health information to a State child support enforcement (IV-D) agency in response to a National Medical Support Notice?" OCR says the privacy rule at 45 CFR 164.512(f) permits a CE to disclose PHI to a "law enforcement official" for law enforcement purposes in compliance with court orders, grand jury subpoenas, or certain written administrative requests. An employee of an IV-D agency meets this definition of a "law-enforcement official," OCR says, and the NMSN constitutes a written administrative request by a law enforcement official. As such, the privacy rule allows a health plan to disclose PHI in response to the NMSN, provided it includes or is accompanied by written assurances by the official that (1) the information sought is material and relevant to a legitimate law-enforcement inquiry; (2) the request is specific and limited in scope; and (3) de-identified information cannot reasonably be used. The CE must also limit the disclosures to the minimum necessary for the purpose, according to OCR, and may rely on the following: (1) the NMSN, or a separate written statement that, on its face, demonstrates that the three assurances required for these disclosures have been met; (2) the NMSN is sufficient to verify the identity and legal authority of the public official requesting the PHI; (3) the NMSN is sufficient as a request from a public official for the minimum information needed to meet the law enforcement purpose of the request.

(2) "Must a covered health care provider obtain an individual's authorization to use or disclose protected health information to an interpreter?" No, according to OCR. "A covered health care provider might use interpreter services to communicate with patients who speak a language other than English or who are deaf or hard of hearing, and provision of interpreter services usually will be a health care operations function of the covered entity as defined at 45 CFR 164.501," OCR says. When using interpreter services, a CE may use and disclose PHI without authorization, in accordance with the privacy rule, in the following ways: (1) When the interpreter is a member of the CE's workforce (e.g., a bilingual employee, a contract interpreter on staff, or a volunteer); (2) when a CE engages the services of a person or entity, who is not a workforce member, to perform interpreter services on its behalf, as a business associate. If a CE has an ongoing contractual relationship with an interpreter service, that arrangement should comply with the privacy rule's business associate requirements. In addition, a CE may, without authorization, use or disclose PHI to the patient's family member, close friend, or any other person identified by the individual as his or her interpreter, OCR says.

***Call 800-521-4323 or visit the MarketPlace at www.AISHealth.com for more information on AIS's detailed* A Guide to Auditing and Monitoring HIPAA Privacy Compliance.**

Some Ambiguities Do Exist

Attorneys have raised some questions about the enforcement notice. For one thing, it may be hard to distinguish privacy and security violations, and a violation of one rule may suggest a violation of the other, says Timonium, Md., attorney Leslie Bender. "How do you distinguish privacy from security complaints? What would be a security incident that would not be a privacy problem? "It seems like there are security risks that are implicitly privacy problems," she says.

And Bell wonders about CMS's right to reject a complaint after a preliminary review. The notice doesn't state criteria for rejecting complaints. Does that mean CMS has "an unfettered right to reject complaints"? For example, when people complain that Medicaid agencies aren't complying with the TCS regulation, can CMS decline to pursue the allegations with no explanation?

It also appears that complainants are up a creek if CMS declines to accept the complaint for investigation. Since HIPAA has no private right of action, complainants have nowhere else to go if they believe a violation has occurred — except perhaps to state court for a common-law action, Bell says.

Contact Bell at mdbell@mintz.com, Hirsch at rhirsch@sonnenschein.com and Bender at lbender@theroi.com. ✧

Training Programs Need to Accommodate New Security Rules

With the security rule going into effect on April 21, hospital privacy officers need to make sure their HIPAA training programs are up to date. *RPP* recently interviewed several privacy officers to learn what modifications they intend to make, or have already made, in their workforce training.

Candace Foster, HIPAA project team leader at ***Deaconess Health System*** in Evansville, Ind., says her facility has been doing computer security training for employees for the past five years. "We also use a knowledge deployment system, which is a Web-based application that we have purchased content for, but we also have built our own content," she tells *RPP*. "We have built security modules — one for those who don't use computers and don't care for patients, but who need to be aware of policies, and a more involved module for those who use computers on a routine basis."

Foster says she also will do a "variety of informal things" such as writing short articles for the hospital bulletin and sending out e-mail reminders "when I spot something that is just a matter of informing people."

At ***Inova Healthcare Systems*** in Falls Church, Va., privacy officer Neschla McCall says all employees at the facility go through some type of security training. "We started drilling down on security training in 2004 and 2005, so we have hit everybody prior to the rule [going into effect], and now we are doing some specialized sessions with IT [i.e., information technology] groups.

IT employees learn about system backup and recovery and access control — items applicable to "people who manage the functions as opposed to the user," McCall says. "The IT department gets more information [than other departments]."

All of the staff is trained on privacy and security during compliance training, McCall notes, and they get mandatory annual refresher courses and reminders. McCall also uses a unique communication system the health system has set up: "We put notes in their paycheck envelopes as things come up that we think we need to emphasize," she says.

Separate Security Training Planned

Henderson Rose is the director of operations at the Danbury Office of Physician Services, a group of oncologists with ***Danbury Hospital in Connecticut***. "Our training for security will be separate from our overall online annual compliance training," he tells *RPP*. "We plan to have something via paper to all staff members by next week and have training complete by [April 21]. We will then incorporate some security into our online compliance/HIPAA training that we normally provide in late spring."

Rose says his staff believes the security training is too important to condense into a larger compliance program. "We followed the same process for privacy, and the staff and physicians were in favor of the separate specialized format," he says.

At the other end of the spectrum, Nancy Prade, privacy officer at the ***University of Colorado Hospital***, says the facility is not undergoing modifications to its training courses now.

"We use [an outside vendor] for courses," she says, referring to online training available for the facility. "We've had both security and privacy covered in the courses since we began so we don't need to modify anything."

Staff members review the information in both the privacy and security rules and link to the hospital's policies, according to Prade. "At the end of the course, they take a test. If they fail, they take the course again," she says.

Contact Foster at (812) 450-7223, McCall at (703) 205-2151, Rose at Henderson.Rose@danhosp.org, and Prade at nancy.prade@uch.edu. ✧

Copyright © 2005 by Atlantic Information Services, Inc. All rights reserved. Reproduction by any means — including photocopy, FAX or electronic delivery — is a violation of federal copyright law punishable by fines of up to $150,000 per violation.

Reporting Problems May Persist

continued from p. 1

"It was clear in the final rule that you can report abuse or neglect," says Kay Love, a program specialist with the Texas Department of Family and Protective Services. "We were very glad the privacy laws continue to allow reporting." But obtaining a child's medical records for an abuse investigation is a horse of a different color. "It was more difficult for us to obtain medical records," she says. But this appears to be caused by providers' HIPAA anxieties or misconceptions, not by an actual privacy rule restraint. State laws on medical records disclosures continue to apply to child-abuse investigations.

The Early 'Fear Period' Is Over

When the privacy rule first took effect two years ago, many child protective services workers had trouble getting access to medical records or eliciting reports in a timely manner, according to people in the field. "Everyone went through a kind of a fear period with HIPAA. There was a lot of exaggeration and misunderstanding," says David Honen, privacy official at the Minnesota Department of Human Services. "A handful of hospitals and clinics and physician offices refused to give information because of HIPAA. County agencies told us they couldn't get medical records in support of a [child abuse/neglect] investigation. Providers said 'because of HIPAA we can't give you this.' But people are largely past that. Once everyone had a firmer grasp on HIPAA and a more accurate reading, it all went away. I don't think [the privacy rule] necessarily impacts on child protection stuff much at all."

Some child protective experts from other states agree that initial problems have largely been resolved. But others do feel that HIPAA is impeding child-abuse reporting and investigations. An organization called HIPAA Government Information Value Exchange for States (HIPAA GIVES) — which "provides a forum for state and county government agencies to discuss and resolve" HIPAA implementation issues — believes that HIPAA is interfering with child-abuse reporting and investigations and increasing potential danger to reporters and social workers, since abusers can find out who reported and/or investigated them. HIPAA GIVES laid out its concerns to OCR in a May 4, 2004, letter, saying that child protective services (CPS) workers often experience the following problems:

(1) "Difficulty in acquiring up-to-date medical information due to resistance of covered entity medical providers to disclose such information without an authorization or court order." HIPAA GIVES says that CPS workers have to investigate to determine whether more intervention is needed to protect the child, which requires repeated access to the child's entire medical record.

(2) CPS workers "are spending much more time and effort obtaining medical records," which increases the danger to the children who are suspected victims of abuse and the risk to CPS workers. HIPAA GIVES says CEs deny medical records to CPS workers pending approval of the privacy officer. "If more than one covered entity is involved, then CPS/APS workers must negotiate various covered entity procedures and documentary requirements," the letter states. Also, the child's personal representative (e.g., a parent of a child patient) has "the unrestricted right" to demand an accounting of disclosures for the child's PHI, which means abusers can find out if they were reported for abusing the child, which "unnecessarily endangers both reporters and investigators."

(3) The CE often reveals the identity of the reporter, either implicitly or explicitly, when tracking disclosures for accounting purposes, "despite state laws that strictly prohibit release of identification of a reporter of suspected abuse or neglect." It appears the privacy rule preempts state laws designed to protect people who report suspected abuse or neglect. "HIPAA GIVES state and county-level members fear this requirement will lead to less reporting of suspicions by medical providers," the letter stated.

HIPAA GIVES asked HHS to amend the privacy rule to exempt CPS disclosures from the accounting requirement, and to "defer to state mandatory reporting, investigation and confidentiality laws pertaining to [child protective services]."

OCR: No Need to Fix What 'Ain't Broke'

OCR claims these amendments are not necessary. It ain't broke, OCR says, so don't fix it. For one thing, the privacy rule is already clear on deference to state law and explicitly allows child abuse-related disclosures to proper authorities. In terms of child protective services needing repeated access to medical records, OCR says that CEs may "continue to disclose to such government authorities repeatedly over the duration of an investigation." Responding to the complaint that abuse investigations are delayed while CEs consult privacy officers about disclosures — putting children at greater risk of harm — OCR notes that Sec. 164.530(a) doesn't say only privacy officers can make discretionary disclosures. "The privacy rule is designed to be flexible and scalable," OCR says.

Finally, OCR states that, when complying with an accounting-for-disclosures request from a suspected abuser, CEs don't have to identify the reporter/investigator. When accounting, CEs have to disclose only the

Call Brenda at 800-521-4323 for rates on bulk subscriptions or site licenses, electronic delivery to multiple readers, and customized feeds of selective news and data…daily, weekly or whenever you need it.

date of the disclosure, the recipient, a brief description of the information disclosed and the purpose of the disclosure.

On its Web site, OCR reiterated the fact that HIPAA does not create obstacles to child-abuse reporting, stating: "Covered entities may disclose protected health information to report known or suspected child abuse or neglect, if the report is made to a public health authority or other appropriate government authority that is authorized by law to receive such reports. For instance, the social services department of a local government might have legal authority to receive reports of child abuse or neglect, in which case, the Privacy Rule would permit a covered entity to report such cases to that authority without obtaining individual authorization. Likewise, a covered entity could report such cases to the police department when the police department is authorized by law to receive such reports. See 45 CFR 164.512(b)(1)(ii)."

Investigations Are a Different Story

It's a different ballgame when it comes to *investigating* child abuse. Obtaining medical records for child-abuse investigations is much harder under privacy laws than reporting child abuse. But again, that's always been the case under state law; HIPAA hasn't changed that, attorneys Annulis and Kristen Rosati say.

"Let's go back in time to January 2003," before the privacy rule took effect, Annulis says. "You have an instance of suspected child abuse, and you report it to a social worker. The social worker asks for additional information. If you gave it to them in January 2003, then you can give it to them now, because the privacy rule was intended not to disrupt state law. If there is a basis [for disclosing PHI] under state law, you can continue to do it."

Since HIPAA defers to state law, the scope of the disclosures turns on the scope of the state law, says Rosati, with the Phoenix law firm of Coppersmith Gordon Schermer Owens & Nelson PLC. "Providers are allowed to report what is required by state law. If state law requires a physician or hospital to report or disclose medical records to child protective services, they are fine under HIPAA. But if the state just requires reporting without turning over medical records, they would have to find a different HIPAA provision to allow turning them over," she says. For example, if there's a law enforcement investigation under way, they can get a court order or grand jury subpoena or present a subpoena. "Without that, providers may not have to turn over medical records. It depends on state law," Rosati says.

But again, that means the *status quo*. Before HIPAA, CPS workers were bound by state law. And since HIPAA took effect, the same rule applies. If the state law allows disclosures, then HIPAA doesn't stand in its way.

For example, according to Texas law, when the state is conservator of a child — which means it has custody — the person or entity (e.g., an emergency room physician) "who reports abuse or neglect has to release to the state any information they have that leads them to believe the child has been abused or neglected," Love says. But if the state doesn't have custody, it will need a court order for medical records. For example, if a neighbor reported physical or sexual abuse and the state wants a medical opinion, it needs a court order for those medical records, she says. All of that remains the same notwithstanding the existence of the privacy rule.

Contact Annulis at brian.annulis@kmzr.com, Rosati at kristen@cgson.com, and Honen at David.Honen@state.mn.us. ✧

HIPAA Security Requires IS Activity Review and Auditing

The following is an excerpt from the chapter on "Security Auditing and Audit Controls" in AIS's comprehensive HIPAA Security Compliance Guide*. It was written by Troy T. Schumacher, CISSP, of Riskology, Inc. in Englewood, Colo. Contact Shumacher at troy@riskology.net.*

The final security regulations require covered entities to know what is happening within their systems that contain electronic PHI (ePHI).

This is spelled out specifically in two standards. "Information System Activity Review," §164.308(a)(1)(ii)(D), requires a regular review of records of system information activity, such as audit logs, access reports, and security incident tracking reports. Also, the "Technical Security Safeguards," §164.312(b), require covered entities to "implement hardware, software and/or procedural mechanisms" that record and examine system activity.

Viewing these two standards together, it is clear that covered entities must have the technology or procedural mechanisms to generate data on system activity and must create policies and procedures to ensure that the review of the information occurs on a regular schedule.

Clearly, the appointed security official must ensure that someone is responsible for regularly reviewing defined audit logs, access reports, and security incident tracking reports. A covered entity should have a policy that defines the time period for regular review of audit trails.

Copyright © 2005 by Atlantic Information Services, Inc. All rights reserved. Reproduction by any means — including photocopy, FAX or electronic delivery — is a violation of federal copyright law punishable by fines of up to $150,000 per violation.

Establish Log Policies

The covered entity should also identify which audit logs will be maintained and reviewed. It is often not appropriate to maintain and monitor all audit logs a system can generate, as this would be overwhelming. The logs to maintain and review are generally defined during the risk assessment process and are an integral part of risk management, also a HIPAA mandate.

Reviewing audit trails requires resources, time, and tools. Keep in mind the type of tools or processes (which could be manual) will depend on the size of the organization. A small provider's office, as an example, will not likely spend several thousands of dollars on an audit tool because of its size and the nature of its business.

As you develop policies and procedures to comply with HIPAA's security rule, keep auditing in mind and ask the following questions with regard to each policy:

(1) Are audit trails an intimate part of the policy and should they be? If they should and are not, clearly there is a problem.

(2) What kind of audit trail is produced as part of the procedure (e.g., electronics, sign-in log, etc.)?

(3) Who is accountable for regularly reviewing the audit trail?

(4) Are tools available to help expedite the process as well as reduce human error in reviewing them, and are the tools appropriate for the organization?

(5) What is the escalation process in the event that noncompliance is determined through reviewing the audit trail?

(6) How long are the audit trails to be backed up and archived (i.e., one year is a good rule of thumb)? Keep in mind that a record of security incidents needs to be maintained for six years per the HIPAA security rule.

(7) What controls (if any) are in place to inhibit someone from unauthorized modification of the audit trails themselves?

(8) Will someone be providing an overall annual audit of these audit trails to determine whether they continue to provide the information the covered entity needs and address noted risks that need to be mitigated by the organization?

Auditable Administrative Requirements

Because audit trails depend upon user identity and levels of authorization, access controls are the prerequisites for monitoring users on the system. In the final security regulations, the importance of access controls to the protection of ePHI is clear: Access control appears as a standard in each type of safeguard. Without access controls, covered entities would not be able to monitor entry into or activity in its information systems.

The administrative safeguards include as their fourth standard in §164.308(a)(4), information access management. This standard requires the covered entity to create policies and procedures to authorize access to ePHI in a way that complies with the requirements of the privacy and security rules.

The addressable implementation specifications in §§164.308(a)(4)(ii)(B) and (C) request policies and procedures that define levels of access for all personnel with regard to the PHI they will have access to and the method and/or means of access. The covered entity also must implement policies and procedures to document initial access, review of access, and modification of the access. All these controls potentially can tie in to your audit program.

Auditable Physical Requirements

Physical access controls are also addressed in §164.310(a)(1) of the HIPAA security regulations. The emphasis here is on proper and timely access to facilities and equipment. The physical considerations for access control are equally important as their electronic counterparts. Note that even for physical access control, the covered entity must:

(a) Specify who has access to designated areas within the covered entity;

(b) Create an authorization process to grant access to specific areas where specified sensitive information or computer hardware is stored; and

(c) Create audit trails that are regularly consulted to detect any unauthorized physical access. The complexity of such audit trails will depend on the size and complexity of the organization.

Auditable Technical Requirements

The technical safeguards in §164.312(a) impose upon the covered entity the responsibility to implement the technical aspects of access control to conform to the access authorization policies and procedures. The two required implementation specifications are:

(1) *Unique user identification:* Assign a unique name and/or number for identifying and tracking user identity. This also holds true for network and system administrators as well as all other employees and management.

(2) *Emergency access procedure:* Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency. For emergency access procedures, there usually is a variance in policy to permit immediate access by authorized individuals to large amounts of information. Because of the nature of this access procedure, audit trail information is extremely important.

***Call 800-521-4323 to receive free copies of four AIS newsletters,* Report on Medicare Compliance, Medicare Advantage News, Drug Benefit News *and/or* Inside Consumer-Directed Care.**

The second standard under technical safeguards in §164.312(b) requires covered entities to do the following:

Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI. For most larger organizations, that means configuring software logging capabilities to monitor users on the system. And in complex organizations, it will be necessary to acquire programs that will help parse the voluminous logs that will be created.

Configuring Audit Logs

An audit trail is an automated or manual set of records providing documentary evidence of user activity. What level of audit trail does your application provide? Is it sufficient to track down anomalies and unauthorized accesses? Covered entities should define the scope and content of an audit trail to balance the necessary security with impact on performance and other costs. Much of this is defined during the risk assessment portion of a covered entity's HIPAA compliance activity.

Because the purpose of an audit trail is to identify what events occurred and who or what caused them, the record should contain the following information:

- The type of event and its result
- When the event occurred
- The user ID associated with the event

PATIENT PRIVACY COURT CASES

This monthly column is written by Rebecca C. Fayed of the Washington, D.C., office of Epstein, Becker, & Green, P.C. 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. Call Fayed at (202) 861-1383.*

◆ **A New York court ordered the plaintiff in a medical malpractice case to sign HIPAA authorizations.** Defendants in a medical malpractice case argued that the court should compel the plaintiff to sign HIPAA authorizations permitting them to meet with the plaintiff's subsequent treating physicians to determine if the physicians' testimony would be necessary at trial. According to the New York Supreme Court, Monroe County, "[i]t has long been the rule **in** New York that defense counsel may interview a plaintiff's nonparty subsequent treating doctors after the discovery phase of litigation.... HIPAA itself provides no impediment to the relief sought by defendants." While the court went on to note that HIPAA permits disclosure of protected health information in the course of judicial or administrative proceedings, it acknowledged that "it is debatable whether a private interview against plaintiff's wishes with his or her physician constitutes a 'judicial or administrative proceeding' sufficient to allow the interview to take place absent an express authorization by the patient." However, the court also stated that "a plaintiff should not be allowed to simply refuse to provide an appropriate authorization to defendants yet seek to interview these same health care providers for potential trial testimony." This being the case, the court ordered the plaintiff to sign HIPAA authorizations permitting defendants access to subsequent treating physicians subject to certain conditions the court set out. (*Steele v. Clifton Springs Hospital and Clinic)*

◆ **A Florida court found that an employee was entitled to unemployment benefits despite the employer's claim of HIPAA violations.** Smith, a certified nursing assistant, questioned the treatment decisions made by a licensed practical nurse with whom she worked and discussed the issue with other nurses at the facility. The facility discharged Smith for spreading rumors about how the other nurse handled patient care and argued that her statements violated the employer's Code of Ethics and HIPAA regulations. The appeals referee found that Smith's comments violated the employer's Code of Ethics and HIPAA regulations, that the employer had discharged her for misconduct connected with work, and that she was not entitled to unemployment benefits. The District Court of Appeal of Florida, acknowledging that there may be times when misconduct is serious enough to warrant discharge, but not sufficient to support denial of unemployment benefits, found that statements made to co-workers concerning the standard of care for a patient does not alone merit a denial of unemployment benefits. In fact, according to the court, "[h]er concerns and comments expressed to coworkers do not transgress the employer's concern that staff not discuss an individual's care with others not involved. One could view her concern and questions for a dying patient's care as commendable." *(Smith v. Unemployment Appeals Commission and Mease Manor, Inc.)*

◆ How the event was initiated (e.g., command, program)

System-level audit trails typically are used to monitor the overall operating system. This audit trail should capture information, such as:

◆ Any logon attempts (whether successful or not);

◆ The date/time of each logon;

◆ The date/time of each logoff; and

◆ The functions performed while logged on (successful or not).

The application log contains information, warnings, and errors about programs and services running on the system. As you set policies, you can also set logging capabilities to capture violations of your policies. ✧

PRIVACY BRIEFS

◆ **CMS has published an article on the HIPAA security rule that focuses on the physical safeguards required to protect electronic health information "from natural and environmental hazards and unauthorized intrusion."** It is the third in a series of seven CMS educational papers that will address the rule's requirements. "When evaluating and implementing these standards, a covered entity must consider all physical access to EPHI. This may extend outside of an actual office, and could include workforce members' homes or other physical locations where they access EPHI," the paper says. The report has sections on facility access controls, workstation use, workstation security, and device and media controls. View the paper at www.cms.hhs.gov/hipaa/hipaa2/education.

◆ **Fox Systems Inc., a Scottsdale, Ariz.-based health care consulting firm, says it has been awarded a five-year contract by CMS to serve as the National Provider Identifier (NPI) enumerator contractor.** Fox's role is to process applications from providers and assign the new national standard provider identification number in accordance with the provisions of HIPAA. The NPI must be used by providers and health plans for all electronic HIPAA compliant transactions by May 23, 2007, Fox says. Visit www.foxsys.com.

◆ **Kaiser Permanente Health Plan notified 140 northern California enrollees that a former employee posted links to their protected health information on her Web log.** According to Kaiser spokesperson Matthew Schiffgens, most members had contact information posted, but for a small percentage, lab test results were made public. The former employee denies posting PHI. Shiffgens adds that the HHS Office for Civil Rights notified the insurer of the breach in January 2005. Kaiser Permanente filed a cease-and-desist order against the employee in California state court. Alameda County Superior Court Judge James Richman ruled that the defendant has until March 23 to show why she made the data public. Schiffgens adds that Kaiser Permanente expects to sue the defendant for breach of contract. Call Schiffgens at (510) 987-3900.

◆ **The National Institute of Standards and Technology (NIST) in March released its final version of "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule," (Special Report 800-66).** NIST says the report summarizes the HIPAA security standards and explains some of the structure and organization of the security rule. It also helps to educate readers about security terms used in the rule and to improve understanding of the meaning of the security standards set out in the rule. View the publication at www.hipaadvisory.com/regs/finalsecurity/nist/800-66.pdf.

◆ **Less than a third of the nation's hospital emergency and outpatient departments use electronic medical records, and even fewer doctors' offices do,** according to a March 15 report by the Centers for Disease Control and Prevention (CDC)**.** About 31% of hospital emergency departments, 29% of outpatient departments and 17% of doctors' offices have electronic medical records to support patient care, CDC reports in its ambulatory medical care surveys that were conducted from 2001 to 2003. "The use of electronic records in health care lags far behind the computerization of information in other sectors of the economy," the agency says. In health care, billing applications were the first to be computerized. Electronic billing systems are used in three-quarters of physician office practices, but computerization of clinical records has been much slower, CDC asserts. Visit www.cdc.gov.

Call 800-521-4323 or visit www.AISHealth.com to order a 30-day free trial review of AIS's comprehensive looseleaf* HIPAA Security Compliance Guide *(with quarterly updates and newsletters).

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 Brenda 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.)