

PATIENT PRIVACY

Practical News and Strategies From AIS's HIPAA Compliance Center

Contents

- 3** 'Accounting for Disclosures' Burden Grows With ARRA Changes
- 3** CVS Pays \$2.25M in Privacy Settlement, Enhances Waste Disposal Policies
- 4** Effective Dates for Privacy, Security Provisions in ARRA
- 6** New HIPAA Amendments Restrict Certain Rx Marketing Practices
- 8** Stimulus Law Will Not Help HIPAA's Negative Impact on Research
- 10** Patient Privacy Court Cases
- 12** Privacy Briefs



Access past issues of RPP, key documents, and 30 narratives on privacy and security compliance at www.AISHIPAA.com. If you don't have a Web site password, call 800-521-4323 or e-mail customerserv@aispub.com. Please whitelist aishipaa@aispub.com to ensure e-mail delivery.

Editor

Eve Collins

Contributing Editor

Neal Learner

Executive Editor

Angela Maas

Special Issue

HIPAA Privacy and Security Provisions in New Stimulus Law

This issue of RPP includes coverage of four major HIPAA provisions in the American Recovery and Reinvestment Act of 2009 (ARRA): (1) the new federal breach notice law, (2) tighter rules on PHI and marketing, (3) accounting for disclosures in electronic health records, and (4) new business associate provisions. The April issue will explore more of these major changes, including new minimum necessary standards, fundraising prohibitions, penalties for noncompliance, and increased enforcement. The full text of these provisions are posted on your subscriber-only Web site at www.AISHIPAA.com, where extensive revisions in narrative sections will be made in coming months to provide subscribers with updated compliance guidance. To receive your user name and password, call customer service at 800-521-4323 or e-mail www.customerserv@aispub.com.

New Federal Breach Notification Provision Exceeds all States' Disclosure Mandates

Covered entities (CEs) that suffer breaches of unsecured protected health information (PHI) will now have to self-report to local reporters (and HHS) if more than 500 individuals in their state are affected, one of the more onerous new privacy and security provisions included in the ARRA.

Forty-four states and the District of Columbia already have security breach notification laws, which to one degree or another require notice to patients and consumers and sometimes to state agencies. But the new federal law appears to be tougher than all of them, and the requirement to alert the media is just one example of why.

continued on p. 8

Business Associates Will Soon Be Subject to Same Rules, Fines as CEs Under New Law

One of the most eye-opening provisions in the health information technology portion of the ARRA, known as the HITECH Act, amends the business associate (BA) provisions in HIPAA to make vendors that work with covered entities subject to the same requirements as CEs. While many agree the change was needed, it may put BA contracts under the microscope all over again, consultants who work with CEs tell RPP.

"I am very pleased with the changes, but I think they will be received begrudgingly by business associates," says Abner Weintraub, president of The HIPAA Group, a consulting firm that works with CEs. "This has been one of the biggest loopholes in locking down PHI." Prior to the changes, BAs were subject only to claims filed by CEs in civil court, he explains, but these changes make them subject to HIPAA enforcement as well (see box, p. 4).

continued

"These provisions are a real game changer for BAs," agrees Reece Hirsch, a partner in the San Francisco office of Sonnenschein Nath and Rosenthal LLP. "It radically changes or expands their legal obligations. I would imagine that many BAs are going to have to take some significant steps to enhance their formal security compliance programs," he says.

BAs now are required to meet the security rule's administrative and technical safeguard requirements. That means creating written policies and procedures, doing risk assessments and hiring a security official. They also will be subject to new breach notification requirements included in the HITECH Act (see story, p. 1).

The approaches to security rule obligations for BAs and privacy rule obligations differ, Hirsch points out. "Under the privacy rule, they take a different approach because the HITECH provisions say that they only have to comply with the BA agreement, and if [BAs] breach that, they are subject to enforcement. It adds teeth to the existing contract obligations," he says. BAs do not have

to meet the other privacy rule requirements such as hiring a privacy official, he notes.

Although CEs were not responsible for monitoring BAs' daily activities, they were ultimately responsible for the PHI entrusted to the vendors, Weintraub explains. This was spelled out in BA agreements. "Now that has changed, and I think that CEs will probably get a little comfort from the fact that BAs have a higher security standard to meet," he says. "I think this was necessary because the security standards really are just the minimum floor of what are considered to be reasonable practices for protecting confidential information."

One thing clarified in the new law is that BAs are now required to notify CEs about a breach within a reasonable time frame and no later than 60 days, points out Frank Ruelas, director of compliance and risk management at Maryvale Hospital in Phoenix. "I certainly can see where covered entities, given the notifications that are now required, are likely going to want to push for as early a notification by its [BAs] as possible," he says.

Ruelas also points out that CEs' former role as educator to BAs on HIPAA's security requirements is diminished now that the provisions also apply to BAs under the HITECH Act.

BA Agreements Under Review?

But CEs may still have some work to do if they have to redo their BA agreements. "The fact is that BAs will have to comply with the security rule's requirement for handling PHI and locking down their own internal systems. That is supposed to be reflected in BA agreements," Weintraub points out.

"This raises a big question because larger organizations have hundreds or thousands of BA agreements, so that's not very appealing to CEs," agrees Hirsch. CEs could benefit from some additional guidance here," he says. Also, "there is a question as to whether requiring amendment [to BA contracts] is really necessary because the...changes apply as a matter of law. So arguably, that is going to apply anyway, so is it really necessary to amend BA agreements to acknowledge that?" he says.

CEs probably will be looking for some tangible assurance that BAs are complying with their new obligations, which could come from amending the BA agreement, says Ruelas. "It can be relatively straightforward in that the business associate agreement simply indicates to the covered entity that it complies with state and federal laws to include those applicable to the business associate under the HITECH Act," he says. Ruelas notes that many of the contracts already do this, so some CEs may not have to worry about it.

Hirsch adds that there is a chance of potential increased liability for CEs. "There is a provision in HIPAA

Subscribers to **AIS's HIPAA Compliance Center** receive **Report on Patient Privacy** (ISSN: 1539-6487), which 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 © 2009 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.

Editor, Eve Collins; Contributing Editor, Neal Learner; Executive Editor, Angela Maas; Publisher, Richard Biehl; Marketing Director, Donna Lawton; Fulfillment Manager, Gwen Arnold; Production Coordinator, Russell Roberts

Call Eve Collins at 800-521-4323 with story ideas for *RPP*.

In addition to **Report on Patient Privacy**, subscribers to **AIS's HIPAA Compliance Center** have access to www.AISHIPAA.com, with archives of past issues of the newsletter, links to government documents, and 30 searchable narratives written by experts in privacy and security compliance. Subscribers receive e-mail notification when a new issue of **Report on Patient Privacy** is posted on the Web site. Please whitelist aishipaa@aispub.com to ensure e-mail delivery.

To order **AIS's HIPAA Compliance Center**:

- (1) Call 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* \$429
 Bill Me \$404

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

that says if you are a CE and you get knowledge of the activity of a BA that is violating the agreement, you have to correct the behavior or terminate the contract. If termination is not feasible, then you have to report the problem to HHS," he explains. "The HITECH Act flips that so that the BA now has the same responsibility. So if a BA finds that the CE is violating the agreement, the BA also is responsible [to report it]," he says.

Vendors Are Not the Only Targets

The BA changes also affect entities that have not fit squarely in the BA category, such as regional health information organizations and health information exchanges. And it affects personal health records (PHR) vendors that didn't exist when HIPAA was first passed. These are organizations that transmit data, but don't always access it, explains Hirsch.

"The exposure risk that [PHR] organizations have is tied to the quantity that they store or use. For PHR vendors not to be considered [BAs] would have been a huge mistake because of the liability and consumer risk

for vendors," says Weintraub. The number of "breaches that have occurred over the last few years is huge.... If you look at sites that track this, [breaches] are into the tens of millions of individual records compromised or breached," he says.

Contact Hirsch at rhirsch@sonnenschein.com, Weintraub at abner@hipaagroup.com and Ruelas at frank@hipaabootcamp.com. ✧

'Accounting for Disclosures' Burden Grows With ARRA Changes

The health information technology portion of the ARRA may offer incentives for providers to begin using electronic health records (EHRs), but it did not come without some give and take. The law strives to make interoperable health information technology available across the country by 2014 partly through the use of bonus Medicare reimbursements to get providers to adopt EHRs. But rules on how CEs account for

CVS Pays \$2.25 Million in Privacy Settlement, Enhances Waste Disposal Policies

CVS Caremark Corp. will pay the government \$2.25 million and enter a corrective action plan after an investigation into the company's disposal of pill bottle labels containing patient information that potentially violated HIPAA, HHS said Feb. 19.

This is only the second agreement and corrective action plan to come out of an alleged privacy violation, and HHS called neither settlement a "fine" or "penalty." The first involved Providence Health & Services in Oregon, which paid \$100,000 and entered a three-year corrective action plan after it lost unencrypted laptops and backup data with information on more than 380,000 patients (*RPP 8/08, p. 1*).

Media reports in 2006 described different pharmacy chains in several cities throwing records into unsecured dumpsters (*RPP 1/07, p. 12*). CVS says in a Feb. 18 statement that the incidents were inadvertent and inconsistent with the company's waste disposal procedures.

The company adds that, soon after the reports surfaced, it enhanced its disposal policies and training programs and instituted a shredding program for documents containing confidential information. CVS says it denies wrongdoing and settled the matter to avoid costly legal proceedings.

This action was the result of a joint investigation by the Federal Trade Commission (FTC) and the HHS

Office for Civil Rights (OCR). The inquiry found that "CVS failed to implement adequate policies and procedures to appropriately safeguard patient information during the disposal process" and "CVS failed to adequately train employees on how to dispose of such information properly," HHS says.

The settlement and corrective action will apply to all of the company's 6,000 retail pharmacies and will be in place for three years. A consent order with the FTC requires monitoring for 20 years, HHS explains.

Along with the announcement of the settlement, OCR posted frequently asked questions (FAQs) about the disposal of protected health information (PHI) on Feb. 18. One FAQ asks, "May a covered entity dispose of protected health information in dumpsters accessible by the public?"

"No" is the short answer, unless the PHI "has been rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed prior to it being placed in a dumpster," OCR explains.

Some other FAQs cover hiring business associates to dispose of PHI, and the reuse and disposal of computers and other electronic media.

Read the agreement with CVS and the FAQs at www.hhs.gov/ocr/index.html.

disclosures in EHRs will be a burden to many organizations.

Accounting for disclosures has long been a thorn in the side of CEs. HIPAA required that providers log when protected health information (PHI) is disclosed for purposes other than treatment, payment or health care operations. This not only was a burden on already busy employees, but has often seemed unnecessary because patients rarely ask to see the accounting.

The changes mandated in the ARRA dictate that providers log all disclosures made through EHRs — including those made for treatment, payment and health care purposes. There will be regulations on this to clarify exactly what information must be maintained in the accounting, notes Reece Hirsch, a partner in the San Francisco office of Sonnenschein, Nath and Rosenthal LLP. He also points out that there is a grace period for complying with these new rules: For CEs that acquire EHRs after Jan. 1, 2009, the rules apply to disclosures made on Jan. 1, 2011, or the date EHRs were acquired, whichever is later; CEs that began using EHRs before Jan. 1, 2009, have until Jan. 1, 2014, to comply.

The amount of work involved in this used to be in the documenting of all the disclosures, which takes a lot of time, especially at larger institutions, says Chris Apgar, president of Apgar and Assoc., an information security consulting firm. But preparing the actual accounting of disclosures for a patient's review is not common. "CEs

are asked to keep this information, but they are not often asked for it," he says.

But now, if medical practices or hospitals have EHRs in place, they are supposed to turn on their audit logs to account for each time a staff member looks at a patient's information. "The problem is putting that data in an easy-to-read format because it will have to have the user's login ID, what they looked up and [why]," says Apgar. "So that is going to require some programming and work on the part of EHR vendors to create functionality."

Apgar also points out that the act of accounting for the disclosures may not be the worst part, but explaining to patients what each staff member does could be cumbersome. There are two sides to the argument here, he says. One is that everyone should be accounted for, so if anyone accesses the record — even for treatment, payment and health care operations purposes — patients should know about it. But the other side of that is that the record is going to be accessed by "a whole host of folks," especially in the hospital setting, Apgar says.

"It certainly seems as if this would be very burdensome," Hirsch agrees. "It seems as if it would require enormous storage capability for those records. I think it will be very difficult to implement," he says.

"It seems like this is a change to HIPAA that doesn't seem to move things in the right direction," Hirsch continues. When the Government Accountability Office issues reports evaluating compliance problems at hospitals, ac-

Effective Dates for Privacy and Security Provisions Contained in ARRA

Unless otherwise specified, all provisions are effective Feb. 17, 2010

PROVISION	SECTION	EFFECTIVE DATE
Breach notification provisions	13402	Effective for breaches discovered 30 days after publication of interim final regulations; HHS must issue interim final regulations by Aug. 17, 2009 (180 days of enactment).
Personal health record (PHR) breach notification	13407	Effective for breaches discovered 30 days after publication of interim final regulations; FTC must issue interim final regulations by Aug. 17, 2009 (180 days of enactment).
Business associates — application of security provisions — application of privacy provisions	13401 13404	Feb. 17, 2010 Feb. 17, 2010
Minimum necessary guidance	13405	Aug. 17, 2010 (18 months after enactment)
Accounting for disclosures: — if used EHR before Jan. 1, 2009 — after Jan. 1, 2009	13405(c)	Jan. 1, 2014 Jan. 1, 2011
Restrictions on disclosures	13405(a)	Feb. 18, 2009
Prohibition on sale of electronic health records/PHRs	13405(d)	Six months after final regulations, which must be promulgated within 18 months of enactment.
Marketing	13406	Feb. 17, 2010 (12 months)
Enforcement for 'willful neglect'	13410	Feb. 17, 2011 (24 months)
Tiered penalties	13410(d)	Feb. 18, 2009
Enforcement by state attorneys general	13410(e)	Feb. 18, 2009

counting for disclosures has been a routine complaint, he says. "There is no seeming benefit from it because so few patients ask for an accounting. I would want to see this relaxed rather than made more stringent."

Not all experts agree with the gloom and doom the new requirements will bring. "I think this is an excellent requirement," says Abner Weintraub, president of The HIPAA Group. "Unless an audit trail is created, piecing one together is nearly impossible," he says.

And "I don't think it will be as much of a burden as some have indicated," Weintraub adds. "It is all electronic...you can sort and collate items...and functions continue to improve. The issue of pulling records together for various purposes is not a big technical hurdle," he says.

Financial Costs May Follow

Apgar says upgrading audit logs to create a record will take programming and, while some hospitals can have their information technology staffs do it, others will have to hire vendors to upgrade their systems, and the vendors will charge the hospitals for that.

Another issue is data retention, he says. One way is to look at the audit logs regularly and retain them for 60 to 90 days. Then destroy the logs, but keep a report about them for six years. Another approach is to keep the logs, but "that is a lot of data to retain," Apgar points out. A happy medium, he says, is to destroy the logs, but extract the information and keep it. This would require that the data be able to be tied to the patient record and would probably have to include information about staff members' jobs and why they would be accessing the record.

"At this time, hospitals need to make sure that functionality is there and will come at a cost. ...Staff members will have to take the time to make sure that all the information is accounted for and respond to patients' requests," Apgar says.

Hirsch points out that many EHR programs already have the capability to keep an accounting of disclosures. So hospitals that already have EHRs may not incur much cost.

Frank Ruelas, director of compliance and risk management at Maryvale Hospital in Phoenix, disagrees that there would be a major cost to CEs. But he points out that the changes say patients can ask for their records in an electronic format, and the costs charged to that patient are to be for labor. What if he or she asks for the records on a magnetic disk, CD or flash drive?

"Who is going to bear the cost of this?" Ruelas asks. "My suggestion is that folks can request this information, but the regulations don't negate that in order for the covered entity to provide the record in an electronic format, the individual is to provide the media. However, if media is going to be used that was obtained by an individual,

the covered entity should give serious thought on how [it] is going to be scanned for viruses or malicious software before it uses such media. Given this risk exposure, it may be easier for the covered entity to buy media in bulk and then use it for such types of disclosures," he says.

Was the Need There?

"I sometimes do wonder about the rationale" behind requiring accounting for disclosures in EHRs, Apgar says. Just from a "practical business perspective," patients don't often ask for them, he points out.

Privacy advocates would disagree with him, he admits. "For things that are outside of treatment, payment, etc., I can understand that. But if you're going to account for every time a record was accessed during a hospital stay, (1) that creates a big record, and (2) it creates frustration because of the confusion of the patient, and the hospital has to explain it," he says.

And what is really gained on behalf of the patient, Apgar asks. "Does a patient gain any additional satisfaction or assurance that [the information] is being used right when a radiologist...or hematologist looked at their record? It was all in the course of treatment," he says.

Ruelas points out that the legislation is pushing standardization of EHRs. "By allowing individuals to get certain information in electronic format, perhaps this will allow for these same individuals to take this electronically formatted information from one health care provider to another, and the recipient provider will be able to upload the information into his or her own electronic health record system so as to promote the care and health care decision making for the individual," he says.

Apgar says sensational headlines may also have contributed to a perceived need, such as when George Clooney's records were accessed last year or news broke that staff looked at Britney Spears's records a few times

How to Comply With New HIPAA Privacy and Security Measures

Join HIPAA attorney **Reece Hirsch**, with Sonnenschein Nath & Rosenthal LLP, for a **March 11** audioconference (CD and print materials available after March 11).

Visit www.AISHealth.com
or call 800-521-4323

over the years. "When there is a VIP, there is added curiosity to look at the record."

"A privacy advocate will say that any time a record is accessed, there should be [an account] of it," Apgar says. "Where that can lead to legal issues and embarrassment is where record is accessed after a patient files a complaint or when the hospital needs to review the charts of a physician....It could open them up for malpractice suits," he says.

Contact Apgar at capgar@apgarandassoc.com, Hirsch at rhirsch@sonnenschein.com and Weintraub at abner@hipaagroup.com. ♦

New HIPAA Amendments Restrict Certain Rx Marketing Practices

New HIPAA patient privacy protections included in the recently enacted economic stimulus package are expected to significantly restrict how stakeholders in the pharmaceutical supply chain — including pharmacies, physicians, health plans and pharmacy benefit managers — gather and distribute prescribing information.

The stimulus prohibits the sale of medical records without a patient's valid authorization. It also, for the first time, applies HIPAA privacy regulations to the business associates of CEs (see story, p. 1). Among other things, the HITECH Act, which consists of the health information technology (HIT) portions of the stimulus, places new limits on previous HIPAA exclusions that had allowed CEs and business associates to furnish "communications" for the purposes of "health care operations," such as case management and communicating information about treatment alternatives. Under the new law, a communication "shall not be considered a health care operation" if the CE "receives or has received direct or indirect payment in exchange for making such a communication." This provision of the law takes effect on Feb. 17, 2010 (see table, p. 4).

The new law is expected to result in major changes to certain pharmaceutical marketing practices. Prior to the HITECH Act, a pharmaceutical manufacturer, without obtaining a patient authorization, could pay a doctor or pharmacy to send prescription refill reminders to patients, as well as pay a doctor or pharmacy to recommend an alternative medication, according to Susan Matthees and Jeff Wasserstein, attorneys at the food and drug law firm Hyman, Phelps & McNamara, P.C.

"However, the HITECH Act limits marketing that is based on protected health information," they explain in a March 2 entry in the firm's FDA Law Blog.

There are several exceptions. According to law firm Sonnenschein Nath & Rosenthal LLP, a communication is no longer a health care operation — and, presumably, is a "marketing communication" that requires an individual's authorization — unless the communication:

- ◆ *Describes only a drug or biologic currently being prescribed for the individual*, and the amount of payment received for making the communication (if any) is reasonable in amount;
- ◆ *Is made by the CE, and the CE has received a valid HIPAA authorization* from the individual to whom it is making the communication; or
- ◆ *Is made by a business associate* and is consistent with the terms of its business associate agreement with the CE.

Under the exceptions, Matthees and Wasserstein note, a pharmaceutical firm can continue to pay for refill reminders, but not for alternative drug recommendations. "This limitation applies to covered entities and business associates, and thus would apply to pharmacies, physicians, health plans, as well as pharmacy benefit managers," they write.

'Definitely a Tightening of Marketing'

While many industry observers point out the law still has to undergo an extensive rulewriting process, one patient privacy advocate says the privacy language could curtail some lucrative pharmaceutical marketing practices. This includes the practice of pharmaceutical manufacturers paying pharmacy chains to gather information about patients who are taking certain medications, including generic drugs, and then having the pharmacy send letters to these individuals urging them to consider taking the manufacturer's own products instead.

"There is definitely a tightening of marketing," says Ashley Katz, executive director of the advocacy group Patient Privacy Rights. "It's been the chain drugstores that have just been wailing and bemoaning how burdensome that is going to be for them, that this is just going to stop their business in their tracks, which I find not true," she tells RPP.

One example of the marketing that this provision could restrict, Katz says, is CVS Caremark Corp.'s mailing last year recommending that physicians "consider prescribing" Merck & Co.'s diabetes treatment Januvia (sitagliptin) when appropriate. The letter, sponsored by Merck, contains a list of the physician's patients — including names, identification numbers and dates of birth — who were taking the generic diabetes drug metformin (RPP 1/09, p. 5). Industry observers say other large pharmacy benefit managers (PBMs) and chain drugstores also send these types of mailings.

This kind of marketing, Katz contends, is worse than if it comes from the manufacturer. "It comes from your pharmacist, which is someone that you know and potentially trust," she says. "But it was paid for 100% by the drug companies pushing their new drug, and not in coordination with the doctor."

The CVS Caremark letter clearly states that funding for the communication was paid for by Merck, and that no personal information was given to the drug maker.

CVS Caremark declined *RPP*'s request for comment on the new law.

Critics: Rx Data Are Still Accessible

Meanwhile, some pharmaceutical industry critics are skeptical that the new law will stop another marketing practice that they contend drives up the cost of drugs. So-called pharmacy "data mining" involves PBMs, pharmacies and other firms gathering and distributing physician prescribing data to pharmaceutical firms for what critics call marketing purposes.

The privacy provisions do not address the issue of prescriber data, says Sharon Treat, executive director of the National Legislative Association on Prescription Drug Prices, a nonpartisan organization of state legislators who have focused on passing anti-data-mining legislation, among other things. In fact, the law's \$2 billion for expanding HIT could actually exacerbate the data mining by providing pharmaceutical sales representatives with more complete prescribing and medical histories of physicians' patients, she tells *RPP*.

"The concern here is that not only does it not limit [access to prescriber data], but the fact that it's electronic makes...it very, very easy to transfer that information," says Treat. "And secondly, the kind of information that is going to be available in that record is going to be far greater than simply prescription information," she says.

Pharmacy data mining now consists only of Rx data, says Treat, a Maine state representative who has sponsored landmark state legislation restricting certain business practices of pharmaceutical firms and PBMs. "So you know that Dr. X has prescribed a particular drug 25 times in the last month," she adds.

"With this electronic record, you'll know that as well as the fact that there were 24 patients who had disease X and one had disease Y, and their histories were the following," she explains. "It won't have the name of that particular patient, but it's going to have all of that other information associated with it," Treat says, noting that such information may be used to develop profiles of individual doctors for marketing purposes.

Some leaders in the pharmacy and PBM industries point to the fact that the government still has to undergo an extensive process of writing rules and regulations for

the law, and that many details are still unknown. They also want to ensure that the new privacy provisions don't hamper the implementation of HIT.

Ensuring That Privacy Doesn't Hamper HIT

The National Association of Chain Drug Stores (NACDS), for example, asserts that the debate surrounding patient privacy has been distorted and, in some cases, is ill-founded.

"Unless a patient gives prior authorization, a pharmacy cannot sell health information that identifies the patient to drug manufacturers for the purpose of helping manufacturers send marketing materials to the patient," Steven Anderson, president and CEO of NACDS, said in a prepared statement before the final stimulus bill was passed. NACDS spokeswoman Chrissy Kopple tells *RPP* that such restrictions have been true under HIPAA as well.

Anderson points out that pharmacies are able to sell de-identified data, which can be helpful for research and quality-assurance purposes, including analysis of health care spending trends for public policy.

Other industry players note that some of the provisions will require changes in business practices.

John Coster, senior vice president of government affairs at the National Community Pharmacists Association, says that contracts between pharmacies and business associates may now require changes.

"Pharmacies are covered entities, but we also have business associates like PBMs or 'switches' that direct the claims to the individual PBMs," Coster says, adding that pharmacies will not be required to enforce the law with these partners. "But some of the security and privacy provisions will apply to business associates in the same way they apply to covered entities." These and other provisions will result in operational changes that will require resources and additional costs over the next few years, he says.

Mark Merritt, president and CEO of the PBM trade group Pharmaceutical Care Management Association, says the key to this legislation is making sure that "the tail doesn't wag the dog" when implementing HIT, including e-prescribing. Merritt says e-prescribing served as the foundation for policies around broader HIT utilization. "The goal ought to be protect privacy, but do so in a context that does not discourage adoption whatsoever," he says. "The question will be, 'What's going to work for providers, not what's going to work for advocates for groups who are not health care folks.'"

Contact Kopple at CKopple@NACDS.org, Coster through John Norton at jnorton@ncpanet.org, Treat at (207) 242-8558 and Katz at akatz@patientprivacyrights.org. ✧

Stimulus Law Will Not Help HIPAA's Negative Impact on Research

Hopes that lawmakers would "fix" the problems HIPAA has wrought on research will have to wait until Congress takes up health care reform later this year. The stimulus law passed last month imposes new requirements that will impact research institutions as much as other CEs. These are on top of the old rules that have plagued researchers and are detailed in two high-profile reports released before the stimulus passed.

Like other CEs, research institutions will be subject to changes in the new law that affect business associate agreements, that require notification of data breaches, and that affect accounting for disclosures.

Just 10 days before the final version of the measure passed the Senate Feb. 10, a committee impaneled by the Institute of Medicine (IOM) issued a scathing report, which urged Congress to exempt research from the rules and impose an entirely new system, or at least make significant changes in the current requirements.

The IOM report also urged research institutions to beef up their data security protections immediately. This report came on the heels of the Jan. 23 report by the Association of Academic Health Centers (AAHC), which urged policy makers and legislators to take similar steps to shield research from the rule (*RPP 2/09, p. 1*).

The IOM committee has been researching the effect of the privacy rule for two years and reached the same conclusions as AAHC, but it suggested two approaches to correcting the situation, one being more radical than the other.

Congress could exempt research entirely from HIPAA, IOM found, and instead implement a new "framework" that would replace the privacy rule and presumably the Common Rule as well, which governs federally funded research involving human subjects.

According to IOM, what the new approach "should do" includes:

- ◆ *Apply to any person, institution, or organization* conducting health research in the United States, regardless of the source of data or funding.

- ◆ *Make a clear distinction between the privacy considerations* that apply to interventional research and research that is exclusively information-based; facilitate greater use of data with direct identifiers removed in health research; and implement legal sanctions to prohibit unauthorized re-identification of information that has had direct identifiers removed.

- ◆ *Require ethical oversight of research* when identifiable health information is used without informed consent. HHS should develop best practices for oversight that

should consider: (1) measures taken to protect the privacy, security, and confidentiality of the data; (2) potential harms that could result from disclosure of the data; and (3) potential public benefits of the research.

- ◆ *Certify institutions that have policies and practices in place* to protect data privacy and security in order to facilitate important large-scale, information-based research.

If its framework is not selected, the government should make a number of changes in the current regulations and issue guidance to help universities and others comply, the committee said.

Specifically, HHS needs to determine best practices for privacy protections in research; encourage greater use of de-identified data and provide guidance on how to use data agreements that are provided for in the privacy rule; and harmonize the Common Rule with the privacy rule.

IOM committee members said they briefed members of Congress and their staffs on the findings while the stimulus bill was under discussion. It is unclear at this point what impact either study will have now that the bill is law.

Read the IOM report at www.iom.edu/CMS/3740/43729/61796.aspx. ↵

Tough Federal Breach Law Enacted

continued from p. 1

"I call it the shame requirement," Jeff Drummond, a partner with the law firm of Jackson Walker LLP, based in Dallas, says of the media notification.

"The only worry before was that anyone would find out about a breach," Drummond adds. "Now if you have one, you have gone from having to just control the negative publicity to being your own whistleblower."

Notification for 'Unsecured' Data Breaches

One big change from the new law is to impose on business associates (BAs) nearly all the same requirements that CEs must meet (see story, p. 1). The breach notification requirement also will apply to them.

The law requires HHS to issue an interim final regulation within 180 days of the signing of the law (Feb. 17) implementing the provisions of the notice requirement. The requirement for notification applies to breaches discovered "on or after the date that is 30 days after the date of publication of such interim final regulations," so the health care community really has little time to prepare for compliance. Generally speaking, most of the other requirements go into effect Feb. 17, 2010, one year after enactment (see table, p. 4).

A breach is defined in Section 13400 of the law as “the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.”

The law also states that a “covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information...shall, in the case of a breach of such information that is discovered by the covered entity, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such breach.”

This last line about data “retention” was a compromise between those in Congress who felt accidental or fleeting disclosures or first-time offenders should be exempt from the notification requirement, and those who wanted patients to learn of all breaches. But the language is confusing, and HHS will probably need to explain how it will interpret this requirement.

“Unsecured PHI” is defined as that which is “not secured through the use of a technology or methodology specified by the Secretary in the guidance” to be issued by HHS within 60 days of enactment.

Notice Must Describe Mitigation

Such technology and methods are those “that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals” including standards issued by standard-setting bodies, the law states.

However, if HHS doesn’t issue guidance by this deadline, “‘unsecured protected health information’ shall mean protected health information that is not secured by a technology standard that renders protected health information unusable, unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute,” according to the law.

BAs that have breaches must notify the CE, and presumably the CE notifies patients, although this is not entirely clear. Persons must be notified of a breach as soon as possible, but no later than 60 days after the incident has been discovered.

The notice must contain certain information, such as:

(1) *A brief description* of what happened and when it was discovered;

(2) *What type of information was involved;*

(3) *Steps persons should take* “to protect themselves from potential harm resulting from the breach”;

(4) *Steps the CE is taking* “to investigate the breach, to mitigate losses, and to protect against any further breaches”; and

(5) *Contact information* for follow-up information and questions.

There are also requirements about whether to mail or e-mail the notice and what to do if addresses are not known.

According to the law, the specifics on what Drummond calls the “shame requirement” are that “notice shall be provided to prominent media outlets serving a state or jurisdiction, following the discovery of a breach described...if the unsecured protected health information of more than 500 residents of such state or jurisdiction is, or is reasonably believed to have been, accessed, acquired, or disclosed during such breach.”

In addition, notice must also go to HHS “immediately” if 500 people are affected, and if there are fewer, “the covered entity may maintain a log of any such breach occurring and annually submit such a log to the secretary documenting such breaches occurring during the year involved.” Annually, HHS will post a list of breaches and send a report to Congress.

‘Meaningless’ Exceptions?

The first problem is that the new federal definition of breach “is so broad,” says David Ermer, with Ermer & Brownell, PLLC, a health care law firm in Washington, D.C. He adds that “the definition of secured PHI, which is not subject to the breach notice requirement, is oriented toward electronic PHI, secured through a technology or methodology identified in HHS guidance that renders PHI unusable, unreadable, or indecipherable to unauthorized individuals. Health plans from time to time have problems with misdirected explanations of benefits. How would you make an explanation of benefits unusable?”

Drummond agrees. Texas law, for example, addresses only data that are on a computer, he says. “If someone broke into your office and stole your file cabinets, you would not have to disclose that,” he says. Under the new federal law, you would.

The law offers two exceptions under which breaches would not have to be reported. It states that “any unintentional acquisition, access, or use of PHI by an employee or individual acting under the authority of a covered entity or business associate” does not have to be reported if:

◆ “Such acquisition, access, or use was made in good faith and within the course and scope of the employ-

ment or other professional relationship of such employee or individual, respectively, with the covered entity or business associate and such information is not further acquired, accessed, used, or disclosed by any person; or

◆ **Any inadvertent disclosure from an individual who is otherwise authorized to access PHI at a facility** operated by a covered entity or business associate to another similarly situated individual at same facility and any such information received as a result of such

PATIENT PRIVACY COURT CASES

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

◆ **A U.S. District Court in California found that a provider may have violated state law and the constitutional right to privacy by disclosing health information to an employer as part of a fitness-for-duty evaluation.** The plaintiff, Matthew Kina, a former United Airlines storekeeper, filed a claim against the Betty Ford Clinic alleging, among other things, that the clinic violated his right to privacy under the California Constitution as well as California's Confidential Medical Information Act (CMIA). While employed by United, Kina was on extended medical leave for depression. While Kina's own treating physician certified that he was fit to return to work, United required him to undergo a fitness-for-duty evaluation at the clinic. The evaluation included assessments of his psychological and non-psychological health by multiple examiners. The clinic disclosed the results of the assessment to United without Kina's authorization. Kina was subsequently terminated, and he filed suit against the clinic alleging that the information it disclosed to his employer included information that did not relate to his ability to do his job. Thus, he alleged that the clinic violated his constitutional right to privacy and the CMIA.

The clinic filed a motion to dismiss both claims. First, it argued that the constitutional claim should be dismissed because Kina did not have a legally protected privacy interest in the results of a fitness-for-duty assessment, that he had no reasonable expectation of privacy in such information, and that there was no evidence to suggest a serious invasion of a privacy interest. The U.S. District Court for the Northern District of California denied the motion to dismiss the constitutional claim because it found that the clinic's alleged "disclosure of detailed and sensitive confidential medical information to United" involved an individual's right to informational privacy. The court found that the allegations were sufficient to state a claim for a constitutional claim. Second, the clinic argued that Kina's CMIA violation claim should be dismissed because Kina did not

specifically identify the "detailed and intimate" information disclosed beyond his functional job limitations. The court stated that the CMIA generally prohibits a health care provider from disclosing health information without an individual's authorization. The court found that Kina had made sufficient allegations regarding the clinic's disclosure of health information to United to state a claim for a violation of CMIA. Accordingly, the court denied the clinic's motion to dismiss the CMIA claim. (*Kina v. United Airlines and Betty Ford Clinic*)

◆ **An Ohio appeals court found that only health information related to the issues in a case is discoverable.** Plaintiff Groening filed a discrimination action against her employer, Pitney Bowes, alleging that it discriminated against her based on her gender, pregnancies and status of being a mother. She alleged that, as a result, she suffered physical and emotional distress. Pitney Bowes requested that the plaintiff sign an authorization permitting the disclosure of her health information. Groening agreed to the disclosure of health information that related to her claim, but not to the disclosure of unrelated information, including her OB/GYN records. While the lower court ordered her to disclose her OB/GYN records, the plaintiff appealed this order. According to the Court of Appeals of Ohio, under Ohio law, a person's medical records are privileged and therefore undiscoverable. However, if a person files a civil action, the privilege is waived for any records that are "causally or historically related to the issues in that civil action." According to the court, when there is a dispute as to whether certain medical records are related, the court should conduct an in-person inspection of the records to make that determination. Accordingly, the court held that the lower court should review the records to determine whether the information is related, and that only related information is discoverable. (*Groening v. Pitney Bowes*)

disclosure is not further acquired, accessed, used, or disclosed without authorization by any person."

This language is throwing some compliance experts such as Ermer into a tizzy because, as he puts it, "these exceptions really are incidental disclosures under the privacy rule and would not be considered violations." He adds that the "exceptions are meaningless."

"There is no exception for situations where it does not raise an issue of identity theft," such as a misdirected letter or a fax, Ermer says. "If the exceptions had said an unintentional disclosure was an exception, that would have provided a meaningful exception."

Encryption May Increase

CEs that want to take steps now to comply with the notification requirement may wish to consider encrypting as much data as possible, and that seems to be one way to avoid having to announce a breach. Reece Hirsch, a partner with the law firm Sonnenschein Nath & Rosenthal LLP, says he thinks the law is clear in providing encryption as a "carrot" to avoid the stick of self-disclosure of breaches.

"Frankly, I don't think this will add unnecessary notifications," he adds, noting that even if such a notification isn't required by law, entities might choose to anyway "because that might be what your patients reasonably expect you to do."

Drummond echoed those sentiments. "This may scare people [into encryption] who want to avoid having these notifications," he says. Many CEs have resisted encryption because they believe it is a monumental "hassle" that can drive away business because it can slow down the communication process. The notification requirement "may just be the thing that topples them," he says.

Drummond says it's still too early to talk in detail about some of the operational steps necessary to comply with this notification requirement. "There's a not a whole lot CEs or BAs can do now until we see the regulations that will further refine" the law, he says.

Entities may wish to compare their state laws to the federal requirements. State laws can be found here: <http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm>.

For his part, Ermer would like to see HHS issue a "model breach notification notice" to guide the industry.

That might be helpful to organizations that have never had any breaches that had to be communicated to patients, such as Mammoth Hospital in Mammoth Lake, Calif. Greg Young, the hospital's compliance officer, has had his hands full keeping up with notifi-

cations required under the state's laws. He says one positive outcome of the federal law, and the increased penalties for violations, is greater support from his higher-ups.

"Management seems much more agreeable to enforce training requirements related to privacy and security issues," Young says. "We have had extensive training, but there are always those that have excuses not to attend and participate. That seems to be going by the wayside and could be a benefit of new state laws we have and now the expanded HIPAA requirements."

Contact Drummond at jdummond@jw.com, Hirsch at rhirsch@sonnenschein.com and Young at young@mammothhospital.com. ♦

Compliance Resources From AIS

- ✓ *High-Risk Areas in Medicare Billing*, which is packed with "how-to" compliance auditing tools for hospitals and providers that were prepared by experienced compliance consultants from Strategic Management Systems, Inc. See a demo at www.MedicareRiskAreas.com.
- ✓ *Report on Medicare Compliance*, the industry's leading compliance newsletter, with weekly news and insightful analysis of the key compliance problems that lie ahead for the industry.
- ✓ *Medicare Part D Compliance News*, monthly news and strategies on marketing, enrollment, formularies, rebates, claims pricing, and fraud, waste and abuse.
- ✓ *Report on Research Compliance*, a monthly newsletter, weekly e-letters and subscriber-only Web site on conflict of interest, human subjects, scientific misconduct, tech transfer and much more; copublished by NCURA.
- ✓ *A Guide to Complying With Stark Physician Self-Referral Rules*, a comprehensive looseleaf (plus quarterly updates) with practical summaries of the federal rules and separate analyses for hospitals, physician groups and other stakeholders.
- ✓ *49 Steps to Implement Sarbanes-Oxley Best Practices in Private & Nonprofit Health Care Entities*, a highly practical book that identifies and describes steps for adopting consensus best practice standards (includes a free CD with templates).

Visit the AIS MarketPlace at
www.AISHealth.com

PRIVACY BRIEFS

◆ **A Dartmouth College researcher found files from major health care organizations containing tens of thousands of individuals' personal information on Internet-based file sharing networks**, according to an article in the Feb. 22-25 issue of *Financial Cryptography and Data Security*. Researcher M. Eric Johnson says the files were inadvertently leaked, but could lead to privacy violations, medical fraud and financial or medical identity theft. The files contain addresses, Social Security numbers, birth dates and treatment billing information on providers' employees and patients, the article says. Some also contain diagnoses and psychiatric evaluations. Also, "we present evidence, from user-issued searches on these networks, that individuals are working to find medical data — likely for malicious exploitation," it says. Read the entire article at <http://mba.tuck.dartmouth.edu/digital/Research/ResearchProjects/JohnsonHemorrhagesFC09d.pdf>.

◆ **Medical records for 150 patients of two Colorado hospitals were missing briefly, but were soon found**, media reports say. Exempla Healthcare, which owns Saint Joseph Hospital and Lutheran Medical Center, notified patients starting Jan. 14 that their records were lost. The documents contained names, addresses, diagnoses and Medicare and Social Security numbers, reports say. The records were being shipped to two groups conducting compliance checks to make sure the hospitals were meeting Medicare requirements, reports explain. FedEx later reported that it found the records. Exempla said the shipping label had been applied to another package. A spokesperson for Exempla could not be reached for comment. Visit www.exempla.org.

◆ **The average total per-incident cost of data breach incidents in 2008 was \$6.65 million**, says the "U.S. Cost of Data Breach Study" sponsored by PGP Corp. and conducted by the Ponemon Institute. The study examined 43 organizations in 17 industry sectors, including health care. It also found that the largest cost increase in 2008 was loss of business created by "abnormal churn," or turnover of customers. That number has risen by more than \$64 per victim (40%) since the annual study began in 2005. Health care companies experienced the highest churn rate of 6.5%, followed by financial services companies at 5.5%, the study found. These findings "reflect the sensitivity of the data collected and the customer expectation that information will be protected," the groups say in a statement about the study. Of all the incidents, 88% involved insider

negligence. Also, half of the organizations said training and awareness will help prevent future breaches, and 44% have expanded the use of encryption, according to the study. The Ponemon Institute is a privacy and information management research firm. PGP Corp. offers e-mail and data encryption software. Visit www.ponemon.org and www.pgp.com.

◆ **The Minnesota Department of Health's (MDH's) plan to warehouse, track and research the public's health data gives the citizens neither a choice nor a voice**, the Citizens' Council on Health Care (CCHC) says in a Feb. 6 letter to the state agency. Part of the plan involves sending the information to the Maine Health Information Center. MDH got the authority to collect, store, disseminate, etc. patient information without holding public hearings and after the plan was added to a state health care reform bill behind closed doors, CCHC contends. It also says that MDH's intent to access and analyze data over the Internet places the data in harm's way. And, CCHC says, the information had not been de-identified enough. The data still include the discharge date and hour; facility and physician identifiers; diagnoses; medications; pharmacy; and gender, CCHC points out. According to state health reform information, the data will be used for a provider peer grouping system and quality measures program. Visit www.cchconline.org and www.health.state.mn.us.

◆ **The National Institute of Standards and Technology (NIST) released a draft Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)**, it said Jan. 13. The guide will assist federal organizations in identifying PII and determining the level of protection it requires, NIST says. The document also offers safeguards on protecting PII and recommendations on data breach handling. NIST can receive comments on the guide by March 13 at 800-122comments@nist.gov. Read the guide at <http://csrc.nist.gov/publications/drafts/800-122/Draft-SP800-122.pdf>.

◆ **The HHS Office for Civil Rights (OCR) has updated the health information privacy pages on its Web site to make it more user friendly for consumers, covered entities and others looking for information about the HIPAA privacy rule**, HHS said Feb. 10. The site includes new information about medical records, employers, personal representatives and court orders, among other things. Visit <http://www.hhs.gov/ocr/privacy/index.html>.

**IF YOU DON'T ALREADY SUBSCRIBE TO THE NEWSLETTER,
HERE ARE THREE EASY WAYS TO SIGN UP:**

1. Return to any Web page that linked you to this issue
2. Go to the MarketPlace at www.AISHealth.com and click on “newsletters.”
3. Call Customer Service at 800-521-4323

**IF YOU ARE A SUBSCRIBER AND WANT TO
ROUTINELY FORWARD THIS PDF EDITION OF
THE NEWSLETTER 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 PDF editions without prior authorization from AIS, since strict copyright restrictions apply.)