

PATIENT PRIVACY

Practical News and Strategies for Complying With HIPAA

Contents

- 3** Express Scripts Notifies 700,000 Breach Victims As Extortion Expands
- 5** HHS Toughens HIPAA Penalties Under New Enforcement Regs
- 5** Other HITECH Act Enforcement Actions
- 6** CEs Face Penalties For Failing to Detect Privacy Violations
- 7** Data Destruction Is Needed to Comply With Breach Notice Rules
- 8** Cross-Shredding May Become the New Standard
- 10** Patient Privacy Court Cases
- 12** Privacy Briefs

 Five narrative sections at www.AISHIPAA.com have now been updated to reflect new requirements contained in the HITECH Act, and a brand-new section on Security Breach Notification has been added. 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.

Editors

Eve Collins
Liana Heitin

Contributing Editor

Nina Youngstrom

Executive Editor

James Gutman

CMS Asks OCR to Probe Humana's Use Of Enrollment Data for Reform Mailings

CMS has informed Humana Inc., that it should have obtained prior authorizations from its members or from the government before mailing nearly a million health-reform-related letters to individuals whose names and addresses the plan culled from its enrollment records.

As a result of its actions, Humana violated its Medicare agreement, CMS told the plan in an Oct. 16 "notice of non-compliance." CMS spokesman Peter Ashkenaz told *RPP* that his agency also asked HHS's Office for Civil Rights, which enforces the HIPAA privacy and security rules, to investigate whether Humana violated the privacy rule as well.

Privacy advocates say CMS's findings are evidence that the rule was indeed violated, and add that this situation highlights the longstanding need to revisit the concept of what kinds of communications plans are allowed without patient approval under the assumption they fall under the category of "operations."

"It is a privacy rule violation to use patient demographic information in this way without consent," says Deven McGraw, director of the Health Privacy Project at the Center for Democracy and Technology.

As covered entities (CEs) know, the privacy rule generally allows the use of protected health information by CEs and their business associates only for treatment, payment and health care operations (TPO). Other uses are permitted if the patient agrees in advance, by signing a standard authorization that is typically time-limited and must clearly state how the information will be used. Demographic information, such as members' names and addresses, is considered protected health information (PHI).

continued on p. 8

Health Plans Face Privacy Rule Changes Under New Genetic Nondiscrimination Act

On Oct. 7, 2009, HHS issued proposed changes for the HIPAA privacy rule in accordance with the interim final regulations for the Genetic Information Nondiscrimination Act (GINA) of 2008, which were released the same day.

Under the proposed HIPAA changes, health plans will need to carefully explore their underwriting practices — using a new and broader definition of "underwriting" — as well as revise and redistribute their privacy notices.

The proposed modifications to HIPAA essentially do five things:

- (1) Make explicit that genetic information is considered to be protected health information (PHI),
- (2) Prohibit health plans from using or disclosing genetic information for underwriting purposes,
- (3) Revise provisions relating to the notice of privacy practices (NPPs) for health plans that perform underwriting,

continued

(4) Make “a number of conforming modifications to definitions and other provisions of the Rule,” and

(5) Update the definition of a “health plan.”

According to Joanne Husted, a health compliance specialist with employee benefits consulting firm The Segal Company in Washington, D.C., genetic information has always been considered PHI, so that particular point is “only a cosmetic change, not a substantive one.” The major change for health plans, she says, is that they can no longer use or disclose genetic information for underwriting purposes. “Because of that change, there’s a cascading effect. There will have to be some tweaking of HIPAA notices and privacy policies and procedures flowing from that change.”

“Underwriting purposes” is defined by the GINA regs as “including, with respect to group health plan coverage, rules for and determinations of eligibility (including enrollment and continued eligibility), computation of premium or contribution amounts, and application of preexisting condition exclusions.” It is not just related to rating and pricing, but rather includes changing deduct-

ibles or “providing discounts, rebates, payments in kind, or other premium differential mechanisms in return for activities such as completing a health risk assessment (HRA) or participating in a wellness program.”

Husted notes that most people in the industry tend to think of underwriting narrowly — as upping a group rate based on concerns about the health of one person in the group. But now, privacy officers “need to think of underwriting purposes in a very broad sense — it’s not just the price on the policy.”

Under GINA, health plans that use PHI for underwriting — which is all plans except for the public plans, says Husted — have to update their privacy notices to specifically state that they will not use genetic information.

Changes That Are Needed May Be Minimal

Mark Stember, a Washington, D.C., attorney with Kilpatrick Stockton LLP, says that despite using PHI, most health plans were not actually using genetic information for underwriting, “so from an administrative standpoint there’s no change. [The plans] are simply updating their documents to make sure they say the right thing.” As covered entities learned in complying with HIPAA, he says, “it’s all about documentary compliance. If you don’t have your documents in order, you’re technically in violation, even if as a practical matter you’re not operating that way.”

However, Sharon Cohen of Watson Wyatt Worldwide, who is based in Arlington, Va., and works with employers, thinks that some covered entities may be unknowingly using genetic information for things that now have GINA implications based on the broad definition of “underwriting.” She gives an example (which falls under GINA rather than the privacy rule) of a health plan that sends a health coach to follow up about disease management after a health risk assessment. The coach asks a few questions about the beneficiary’s family medical history. While the health coach seems to be providing some type of medical care, which would make the use of genetic information allowable, the service is coming from a health plan. It’s a fine line whether the family history questions are permissible, dependent on when in the enrollment process they were asked and whether they are tied to any kind of incentive. Covered entities should “go through their policies and procedures to make sure they are not in violation of the [underwriting] rule — not just the policies on paper, but the ones really in operation,” Cohen says.

As expected, HHS is still hammering out some of the GINA details, especially concerning timelines. According to the HIPAA privacy rule as currently written, a covered entity must notify beneficiaries of a material change within 60 days of implementing the change. The new

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 © 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.

Editors, Eve Collins and Liana Heitin; Contributing Editor, Nina Youngstrom; Executive Editor, Jim Gutman; Publisher, Richard Biehli; Marketing Director, Donna Lawton; Fulfillment Manager, Gwen Arnold; Production Coordinator, Russell Roberts

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

Subscribers to **Report on Patient Privacy** also receive access to **AIS’s HIPAA Compliance Center** at 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 **Report on Patient Privacy**:

- (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 6% sales tax.

proposed HIPAA modifications state that “the proposed requirement to explicitly include a statement regarding the prohibition represent a material change to the NPP of health plans that perform underwriting,” so the 60-day time frame should apply. And while modifying the document would be simple, redistributing it could be quite a burden. “HHS is not wild about the idea of just telling plans to redistribute privacy notices so they can add five words. They’re considering what to do and asking commenters to weigh in about what they think is appropriate under the circumstances.”

Several Timelines Are Possible

There are several timeline options on the table, says Cohen. HHS could allow health plans to send the new notices with their annual enrollment information, waive the time frame altogether or keep the 60-day deadline. Stember notes that since the original GINA regulations were released in May, many health plans already changed their notices and sent the new ones out with their annual enrollment mailing. For health plans “to change privacy notices midyear it would be a different story because there are specific costs associated with that,” says Stember.

If the privacy notice change does constitute a material change under the final rules, health plans will also need to do employee training, says Stember, though there are no specific requirements in the privacy rule about how and when. Educating staff could be as easy as a one-page memo, he says, or as difficult as a series of training sessions, depending on the company’s evaluation of its needs.

The proposed time frames have potential to cause confusion in light of the changes CEs have to make under the HITECH Act. The security breach notification interim final rules officially went into effect on Sept. 23, though HHS has said it will not enforce these regulations for the first six months (*RPP 9/09, p. 1*).

Covered entities also need to modify their business associate agreements by February 2010 (*RPP 10/09, p. 1*). The proposed changes to the privacy rule state that health plans will be required to comply with the new standards 180 days after the final rule is published. “The good news from the perspective of the HIPAA privacy officer is that nothing has to be done right now — this is one change in the law unlike the rest of it that’s not yet effective,” says Husted. “They’re basically looking at having six months from the time they issue the final rule to get their ducks in a row,” and the final regs aren’t likely to come out until sometime next year.

But wouldn’t it be wise to get a leg up on these changes, since so many other changes will be due right around the same time? Not necessarily. Stember suggests

health plans save time and money by waiting to make the HITECH and GINA changes at once “rather than doing it piecemeal.” The HIPAA final changes are likely to be made before February, so mailings, policy and procedure updates and training sessions can be done at the same time for both regs to comply with both deadlines, he says.

Husted agrees that health plans should wait on making changes for both GINA and HITECH. “They may have to do some HITECH stuff first, but HHS is aware this is all happening. It’s the same office writing the regulations, so I’m sure they’re trying to coordinate. The only thing to do now is breach notification, and CEs should already be doing it.”

Contact Husted at jhusted@segalco.com, Stember at mstember@kilpatrickstockton.com and Cohen at Sharon.cohen@watsonwyatt.com. ✦

Express Scripts Notifies 700,000 Breach Victims as Extortion Expands

More than a year after becoming the target of an extortion plot that resulted in fewer than 200 people being notified that their data were accessed, pharmaceutical benefits manager Express Scripts not only hasn’t cracked the case, but now has proof the perpetrator actually possesses Express Scripts data for at least 700,000 members, some of whom may come from among all of its corporate customers.

Initially, Express Scripts acted as if it was dealing with a small incident when it detailed the extortion demand on Nov. 6, 2008 (*RPP 12/08, p. 1*). At the time, it said the extortionist had sent a letter including names, dates of birth, Social Security numbers and some prescription drug information for 75 “members” of its drug benefit plans. Last year, it did say the extortionist had threatened to expose data from “millions.” It also offered a \$1 million reward to help catch the culprit.

On Nov. 11, 2008, it made a second announcement, saying three employers that were Express Script clients — Toyota among them — had also gotten extortion letters. But it still did not expand the number of affected individuals much beyond the initial number, and press reports indicate that in 2008 Express Scripts contacted only a few hundred people.

But that all changed last month, when Express Scripts acknowledged that it had new information that led it to notify an additional 700,000 members whose personal data may have been breached.

“In late August, Express Scripts was informed by the FBI that the perpetrator of the crime had recently

forwarded a letter and data file to a law firm," Express Scripts spokeswoman Maria Palumbo says.

"The data shows that the extortionist possesses more member records from the same period as those identified in the 2008 extortion attempt... [W]e became aware that approximately 700,000 members were affected and required notification," she says. "We have now notified all those members."

Palumbo also tells *RPP* that the 700,000 come from "1,600 clients," which may well be all of its corporate customers, since in 2007 the chief medical officer of Express Scripts testified before a U.S. House committee that the firm had 1,600 customers with more than "50 million lives."

Extortionist Contacted Law Firm

Express Scripts says it learned of the expansion from the FBI, which in turn was tipped off by an unidentified law firm that received a letter and data from the extortionist.

Express Scripts refused to identify the firm except to say it was one that had filed suit against it "earlier this year." That could mean a law firm that had filed suit after its employees found out they were among those who lost data (although no such lawsuit has been reported), or it could be the law firm that filed a class-action suit against Express Scripts, which has been reported.

The class-action suit was filed by a legal team including Finkelstein Thompson, LLP, in Washington, D.C.,

which *RPP* contacted. Karen Marcus, an associate with the law firm, said all of the pleadings in the case, and other related information, are under seal and thus she could not comment. The case is still ongoing, with a decision expected soon on Express Scripts' motion to dismiss, she says.

No New Security Actions Were Taken

Following the first threat, Express Scripts says it "took aggressive action to enhance its security operations and data handling procedures." It has not taken any additional security-related actions, Palumbo says.

The steps it took last year were:

- ◆ Enhanced security monitoring;
- ◆ Tighter Internet filtering to restrict access to Web-based e-mail services;
- ◆ Further restricted access to sensitive data, including limits on generating bulk data reports and access to sensitive data fields; and
- ◆ A ban on the use of sensitive information on unencrypted media and on the use of USB media devices.

Palumbo adds that: "At this time, we have not confirmed any fraudulent misuse of member information as a result of this incident. We continue to offer all members free access to identity consultation, investigation and restoration services through Kroll Fraud Solutions."

But the newest threat shows the perpetrator is still on the loose. Asked if there had been any progress in solving the case, Palumbo could say only that "the FBI investiga-

How to Amend HIPAA Business Associate Agreements to Comply With the HITECH Act: Strategies for Meeting the February Deadline

- What contract language should CEs consider using related to their BAs' compliance with breach notification and the security rule?
- What strategies should CEs consider to effectively manage the onerous task of amending scores (if not hundreds) of BA agreements in the next three months?
- How much time should CEs give BAs to notify them of a security breach, since the CE itself must go public with certain breaches in 60 days?
- What definition of "breach" should CEs give to their BAs? Should it include the "harm" standard or should CEs reserve this determination for themselves?
- To what extent have the HIPAA liabilities of covered entities been lessened with these new obligations for business associates?

Join veteran HIPAA attorney **Reece Hirsch** for an **Dec. 8** audioconference.

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

tion is ongoing, and Express Scripts continues its own internal investigation. Because of these investigations, we cannot provide any additional details at this time."

To date, neither the HHS Office for Civil Rights nor state agencies that regulate data privacy and information breaches have taken any action against Express Scripts, Palumbo said. OCR's policy is not to comment on whether it is conducting an investigation, a spokesman told *RPP*.

Contact Palumbo at MPalumbo@express-scripts.com. ✧

HHS Toughens HIPAA Penalties Under New Enforcement Regs

On Oct 30, HHS released the interim final rule to amend HIPAA's enforcement regulations and ramp up civil monetary penalties as mandated by the February 2009 HITECH Act.

The rule incorporates four tiered ranges of penalty amounts as outlined in HITECH for violations that were brought about unknowingly, due to reasonable cause, due to willful neglect but corrected, and due to willful neglect but not corrected. The new penalties apply to violations that occur on or after Feb.18, 2009.

Previous civil penalties under HIPAA — which were rarely imposed — consisted of \$100 fines per violation with a \$25,000 yearly cap on identical violations (*RPP 4/09, p. 10*). The interim rule, published in the *Federal Register* of Oct. 30, categorizes violations to "reflect increasing levels of culpability" and adds teeth to the fines, as follows:

- ◆ If the violator did not know that he or she violated the law, and would not have known by exercising due diligence, the penalty for an identical violation is at least \$100 and up to \$50,000 for each violation.
- ◆ If the violation was due to reasonable cause, not willful neglect, the penalty is at least \$1,000 and up to \$50,000 for each violation.
- ◆ If the violation was due to willful neglect and was corrected within 30 days of when the CE knew or should have known about it, the penalty is at least \$10,000 and up to \$50,000 for each violation.
- ◆ If the violation was due to willful neglect and was not corrected, the penalty is at least \$50,000 for each violation.

For all tiers, the maximum penalty amount for violations of an identical provision is \$1.5 million per calendar year.

The original language from Section 13410(d) of the HITECH Act includes a \$25,000 cap on identical violations for the first two tiers, and a \$250,000 cap for the third, but HHS modified the language in the interim rule.

As explained in the regulation, "HHS considered the conflicting statutory language that references two tiers of penalties 'for each violation,'" and "with the exception of violations due to willful neglect that are not timely corrected, this interim final rule adopts a range of penalty amounts between the minimum given in one tier and the maximum given in the second tier for each violation," and makes \$1.5 million the ceiling for violations.

HIPAA also had an "affirmative defense" provision for covered entities whose violations were not due to willful neglect. The modified rule strikes this defense, and instead offers an affirmative defense only to those CEs whose violations were not due to willful neglect and were corrected within 30 days of the time the violation was known, or would have been known under due diligence.

HHS issued this interim final rule, which addresses only those enforcement provisions that have already

Other HITECH Act Enforcement

The HITECH Act sparked several other patient privacy enforcement actions that CEs should know about, most of which have yet to become effective.

- ◆ State attorneys general can bring civil actions in federal court on behalf of the state's residents when there is reason to believe residents' interests have been threatened or adversely affected. *Effective Feb. 18, 2009 (RPP 4/09, p. 1)*.
- ◆ Business associates are now directly accountable to federal and state authorities for failure to comply with the HIPAA privacy and security provisions and can face the same enforcement actions as CEs. *Effective Feb. 18, 2010*.
- ◆ Individuals, including but not limited to employees of a covered entity, can face criminal penalties for violating HIPAA if they use or disclose PHI maintained by a CE without authorization. *Effective Feb. 18, 2010*.
- ◆ All civil monetary penalties collected as result of privacy or security violations must be transferred to OCR for enforcement purposes. *Effective Feb. 18, 2010*.
- ◆ HHS is required to formally investigate any complaint of a HIPAA violation if a preliminary investigation indicates the possibility of willful neglect. If the violation is found to constitute willful neglect, HHS must impose a civil penalty. *Effective Feb. 18, 2011*.

taken effect under HITECH, before issuing a proposed rule and without a prior comment period. In the preamble, HHS explains it has “good cause . . . to waive the notice-and-comment requirements” because “many covered entities may be unaware they are currently subject to significantly greater penalties for violations of the HIPAA rules.” The regulation becomes effective Nov. 30, but commenters have a chance to weigh in until Dec. 29.

See the rule at <http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/enfifr.pdf>. ✧

Covered Entities Face Penalties for Failing to Detect Privacy Violations

There’s still a place for voluntary HIPAA compliance, but former privacy enforcement chief Richard Campanelli says it’s a whole new enforcement world with the consolidation of privacy and security in the Office for Civil Rights, the enhanced enforcement requirements and penalties under the HITECH Act, and the empowerment of state attorneys general under HIPAA. The parallel policing activities and interest of the FTC in privacy disclosures also up the compliance ante.

“OCR has shown it’s willing to routinely pursue settlements of significant size and importance,” says Campanelli, who was director of OCR when HIPAA took effect in 2002 and then a counselor to the HHS Secretary until January 2009. However, he notes “the department will continue to exercise its discretion in many cases,” a position that was reiterated in the interim final enforcement regulations unveiled Oct. 30.

Covered entities should brace for the kind of crack-down on privacy and security violations they didn’t face before. For one thing, the HITECH Act and the implementing enforcement regulations strike down “the previous bar on the imposition of penalties if the covered entity did not know and by exercising reasonable diligence would not have known of the violation,” says Campanelli, now with the Washington, D.C., office of the law firm Baker & Daniels. In other words, covered entities won’t be off the hook because they failed to identify confidentiality problems. “That used to be an affirmative defense,” he notes. However, the enforcement regulation also gives providers a little slack. It bars the imposition of penalties for violations that are corrected within a 30-day period (or any extensions granted), as long as the violation was not due to willful neglect.

HIPAA investigations also may become broader now that privacy and security enforcement is consolidated in OCR instead of split between OCR and CMS. “When doing investigations, OCR can be expected to be more thorough and expansive when looking at security violations,” he says. For example, impermissible disclosures

are on the list of OCR’s most frequently investigated complaints. If a covered entity lacks access controls and workforce members can potentially view more PHI than warranted to do their job, the failure to abide by the minimum necessary standard and adopt administrative and technical safeguards and have access controls can potentially play out as both privacy and security violations, Campanelli says.

The HITECH Act’s emphasis on penalizing covered entities that are “willfully neglectful” about their HIPAA responsibilities, which triggers a violation, also poses a threat to covered entities that are too lax about HIPAA. The new enforcement regulation defines willful neglect as “conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated.” Campanelli says an example might be if a covered entity were repeatedly notified (by internal reports or external complaints) that PHI was exposed, and yet did nothing to address the problem. Covered entities face fines of \$50,000 per violation caused by willful negligence, up to \$1.5 million per year (unless the violation is corrected in 30 days).

State AGs Have New Powers

The HITECH Act’s empowerment of state attorneys general is another example of greater emphasis on HIPAA violations, but these officials have already become more active. For example, the Indiana attorney general recently reached settlements with two pharmacy chains, Walgreens and CVS, to resolve complaints that customers’ medical information was improperly discarded in trash bins outside some of the stores. Under the settlements, CVS and Walgreens agreed to “implement extensive employee training, management policies and detailed reporting to provide greater safeguards so that customers’ personal information will not be improperly disclosed,” the Indiana AG’s office stated. The allegations involved 10 CVS and six Walgreen pharmacies. Though the cases were settled under state identity theft laws, the attorney general noted in a statement that disclosing confidential information violates HIPAA, foreshadowing the state HIPAA enforcement to come. OCR eventually settled a privacy issue with CVS. “The OCR’s federal case involving Walgreen Co. is ongoing,” the Indiana AG stated in July.

Given the direct application of HIPAA to business associates, “covered entities and business associates should think through whether they want to clarify whether the business associate is an agent of the covered entity or an independent contractor,” Campanelli says. *The reason:* Covered entities must report their own information breaches and their agents’ breaches as soon as possible, but no later than 60 days after becoming aware of the breach. “Consider making the relationship crystal clear in the contract,” he advises, because if business associates

are agents of the covered entity, reports have to be made, and the clock is ticking.

Notwithstanding the coming enforcement crack-down, many covered entities are generally better equipped to prevent violations, Campanelli says. "For many businesses, HIPAA has become part of their architecture," he says. "They went from having to comply with a new law that was an overlay" to integrating privacy and security protections into their business operations. "The challenge after all these years is for companies and business associates to be more vigilant about compliance. They may have their policies and procedures in place, but are they vigilant about making sure their workforce is trained and aware enough so they are implementing policies and procedures on a continuous basis?" And are adjustments made to account for the direct application of HIPAA requirements to business associates?

Contact Campanelli at Richard.campanelli@bakerd.com. ♦

Data Destruction Is Needed to Comply With Breach Notice Rules

With the HITECH Act's new requirements that patients be notified when there has been a breach of unprotected information (*RPP 9/09, p.1*), covered entities (CEs) and business associates (BAs) may want to rethink their data destruction processes.

HHS released final guidance on rendering data unusable, unreadable and indecipherable in August in its final rule on breach notification requirements (*RPP 9/09, p. 7*). The HITECH Act, enacted in February, mandates that this HHS guidance be updated each year, so CEs and BAs have ample time to get lingering questions answered on both encryption and data destruction.

In the meantime, HIPAA security consultant Chris Apgar advises CEs and BAs to remember that, when protecting or destroying PHI, there are technologies other than laptop or desktop computers that can house PHI. For example, Apgar knows of one vendor who swaps out commercial copiers for companies. Standard machines have one or two hard drives that hold tons of information. "That isn't necessarily something you think about when you get a new machine," he says. Since copiers in CEs and BAs are used to duplicate medical records, those hard drives would need to be formatted, Apgar says. "This [vendor] is now destroying that data and giving organizations a certification of destruction."

Another thing CEs and BAs may not have considered is that there are data stored on devices like MRI machines after they are used to serve patients. If the facility is getting rid of the machine because it's no longer usable, the hard drive should be formatted or erased (i.e.,

degaussing). If it is being moved, all of the patient data should be backed up beforehand, Apgar says.

Many organizations also move older computers that are still usable from one department to another when upgraded equipment comes in. In this case, it is important to make sure PHI is completely removed from the computer, especially if its new home is a department that should not have access to the PHI, Apgar says.

Make Sure Old Computers Are 'Clean'

"People think that if you hit the 'delete' button, information is gone, but that's not true," he says. Hackers have been able to recover data very easily, and some companies charge pretty large sums to do the same. But Apgar says software on the market now allows organizations to "bleach" or shred hard drives and portable media of deleted data by cleaning it and destroying the information. "That's one way of doing it without totally reformatting a hard drive and then reinstalling everything and it's also relatively inexpensive," he says.

Another way to sanitize computers that are being moved is by saving data to the organization's server, so that the work station at most has temporary files, says consultant Frank Ruelas. "When moving computers from one area to another — even in same department — we are seeing a sensitivity to make sure that the computer is clean. We're not seeing people drill holes into old hard drives anymore. Now with availability of software to sanitize,...we can clean media with a high level of confidence that it will not be retrieved and then [equipment] can be used by other folks. Before, the only way to be 100% confident was to make sure it never went anywhere or was completely destroyed, Ruelas says.

Portable media are another problem area, Apgar adds. Many health care professionals are using smartphones today to be accessible anywhere at any time. These devices can hold quite a bit of data and sometimes carry patient records "If they're storing information about patients on their smartphone, there's not always a lot of thought given to that," he says. The flashcards in these devices should be formatted once they're done being used. "Real geeks would do it twice and then fill it with binary code," he contends.

Of course, laptops are often a nightmare for covered entities and business associates, and the risk has increased in recent years with how inexpensive and prevalent they've become, Ruelas points out. "Maybe before, because of the cost, it was upper management [who received a laptop], but now employees up and down the organizational chart can have them, and it's not uncommon even in the physician-practice setting to have one." CEs and BAs need to continue to be vigilant with laptops

because the hard drives are huge and contain much more data than that on a thumb drive or flashcard.

For paper, shredding is always the best option, Apgar says, and CEs and BAs should be using cross-cut or diamond-cut shredders (see box, below). Covered entities that are “going green” can use recycling bins with locks so they can be picked up and taken to the paper pulping plant, he says. Or the CE can make sure that employees are responsibly dumping the small bins under their desks into a larger “confidential” recycling bin. “CVS was a good example of what not to do” when employees dumped prescription labels with PHI in publicly accessible dumpsters, he says.

No matter what the method of destruction, Apgar says each covered entity must have a fully defined policy and procedure in place on getting rid of electronic and paper data. The destruction “needs to be documented, and you need to be policing it to make sure it actually happens,” he says. “From a legal standpoint, if you have a policy and procedure in place and you can demonstrate that it is being followed, the legal risk goes down. A lot of times I’ll conduct an audit, and the facility is doing it right, but is not documenting it,” he explains.

Contact Ruelas at frank@hipaabootcamp.com and Apgar at capgar@apgarandassoc.com. ✧

CMS: ‘Humana Violated Medicare’

continued from p. 1

Humana is a CE under HIPAA and also must follow CMS’s Medicare rules, since it offers both a Medicare Advantage (MA) plan and a stand-alone Part D drug plan.

The letters that came to the attention of both CMS and OCR were included in official Humana envelopes marked “*Important information about your Medicare Advantage plan — open today!*” Inside, the letter, addressed to the beneficiary by first name, states that Humana “is working diligently to ensure that our nation’s leaders understand how proposed reforms might affect you.”

It then asks the beneficiary to do two things:

(1) Opt into the plan’s “Partner” program by sending in the attached postcard by which the member will join some 50,000 other Humana members who are “receiving information on this issue and learning how to get involved to protect your Medicare health plan coverage.”

(2) “Let Congress know why Medicare Advantage is important to you,” directing the enrollee to go to a Humana Web site where an automated letter can be sent to Congress, which is considering “significant cuts” to MA, or to call a phone number to learn more about this.

Cross-Shredding May Become the New Standard

Cross-shredders may soon become the hot new item in an office supply store near you, courtesy of the privacy and security provisions of the HITECH Act.

All shredders use sharp blades to destroy paper documents and electronic media, but unlike standard shredders, which slice their prey into straight lines, cross shredders go a step further and cut PHI into tiny squares or rectangles.

The HITECH Act, which emphasizes rendering PHI unusable and inaccessible, does not explicitly require cross-shredding. And regular shredders were good enough for the initial HIPAA privacy and security regulations.

But in recent months, HHS officials have indicated in speeches that only cross-shredding is a surefire way to demolish PHI past the point of no return, says consultant Virginia Gleason, with AR Systems in Twin Falls, Idaho. And an April 27 HHS guidance on breach notification requirements refers to another government agency’s security guidance that advocates cross-shredding. “Straight-line shredding is no longer seen as a definitive way to destroy PHI,” she says.

Gleason says the idea that there is a true risk of an interloper piecing back together the tiny strips from regular shredding, to the point where only cross-shredding suffices, smacks of paranoia. “Someone has been watching CSI too often,” she says.

When she heard HHS officials talk about the importance of cross-shredding, Gleason says “my eyes rolled back in my head. Shredding is shredding,” she says. “I think someone would have to go to a great deal of work to take a bag of shredded medical records and paste them back together. It doesn’t seem logical that anyone would go to that extent to piece together PHI in any form.”

The destruction of documents is required in the context of the HITECH Act’s breach notification requirement. Covered entities and business associates must notify people if their PHI has been disclosed because “it was not secured through the use of a technology or methodology that renders PHI unusable, unreadable, or indecipherable to unauthorized individuals.”

Encryption and destruction are the two methods deemed appropriate for accomplishing this, HHS

In addition, it states that “leading health reform proposals...include billions in Medicare Advantage funding cuts, as well as spending reductions to original Medicare and Medicaid. While these programs need to be made more efficient, if the proposed funding cut levels become law, *millions of seniors and disabled individuals could lose many important benefits and services* that make Medicare Advantage health plans so valuable.” [emphasis added by Humana]

The letter is signed by Phillip Painter, Humana’s chief medical officer. According to CMS, Humana sent out 900,000 such letters to beneficiaries between Sept. 8 and 11 “in all 50 states, as well as Washington, D.C., and Puerto Rico.”

Sen. Max Baucus (D-Mont.) first called attention to Humana’s letters during the period when the Senate Finance Committee he chairs was working on a health reform bill. After Baucus complained the letters were untrue and a scare tactic, he asked CMS to look into the matter. Teresa DeCaro, acting director of CMS’s Medicare drug and health plan contract administration group, sent Humana a letter on Sept. 18 ordering it to immediately stop all such mailings, and remove similar materials “directed to Medicare enrollees from its Website.”

In her Sept. 18 letter, DeCaro said CMS was “concerned that, among other things, this information is misleading and confusing to beneficiaries, represents information to beneficiaries as official communications about the Medicare Advantage program, and is potentially contrary to federal regulations and guidance for the MA and Part D programs and other federal law, including HIPAA.”

According to Ashkenaz: “The privacy concerns were raised with OCR, and it is up to them to decide what actions they want to take, if any.” OCR’s policy is not to comment on whether it is investigating a CE, although its spokesman told *RPP* to “check back” for updates.

Humana spokesman Thomas Noland said he had no information to indicate whether OCR is investigating the plan. He declined further comment except to say that Humana was “pleased” CMS had resolved its issues with the plan.

CMS’s Oct. 16 notice of non-compliance said Humana committed two Medicare violations. “To the extent that Humana used its Medicare enrollment records for this mailing, this was a violation of your organization’s data use agreement with CMS,” DeCaro wrote. “In this case, the information was not used to provide information about the enrollee’s Medicare

Cross-Shredding May Become the New Standard (continued)

said in its April 27 guidance published in the *Federal Register*. The guidance, which is very brief and requests ideas from the industry, states that paper, film and other hard-copy media must be shredded or destroyed to the point where it can’t be read or otherwise reconstructed.

However, the guidance references “Guidelines for Media Sanitization,” published by the National Institutes for Standards and Technology (Special Publication 800-88). And in that document cross-shredding is considered an essential tool for preserving security. The NIST guidelines state that paper should be destroyed “using cross cut shredders, which produce particles that are 1 x 5 millimeters in size (reference devices on the NSA paper Shredder EPL), or to pulverize/disintegrate paper materials using disintegrator devices equipped with 3/32 inch security screen (reference NSA Disintegrator EPL).”

Also, the NIST guidelines note that “paper shredders can be used to destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assur-

ance in proportion to the data confidentiality that the data cannot be reconstructed. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD) and MO disks, must be destroyed by pulverizing, crosscut shredding or burning. When material is disintegrated or shredded all residues must be reduced to nominal edge dimensions of five millimeters (5 mm) and surface area of twenty-five square millimeters (25 mm²).”

The fact that HHS refers to the NIST paper reflects the HITECH Act’s — and HHS’s — greater specificity than HIPAA in prescribing the methods for achieving privacy and security.

Gleason says the latest sign that PHI must now be pulverized is that “there are a lot of office equipment manufacturers that are now advertising that their cross-shredders meet HITECH requirements.” In light of these developments, she recommends that covered entities “slowly but surely replace their regular shredders just so there is no question.” But she emphasizes “slowly,” especially as covered entities await more guidance from HHS.

Contact Gleason at viriniagleason5@msn.com. ✦

plan, but instead was used by Humana to provide information related to their health care reform outreach efforts," CMS told the plan.

The second infraction, CMS said, relates to marketing. CMS deemed the letters marketing materials, which are to be reviewed and approved by CMS prior to distribution. The letters did not follow this process.

CMS itself drew another parallel to the privacy rule. Simultaneous with the non-compliance letter, CMS issued "guidance" clarifying mailings to enroll-

ees, and DeCaro warned Humana in her letter to the plan that the agency "may take additional compliance or enforcement action, including the possible imposition of intermediate sanctions or civil monetary penalties." The guidance applies to all Medicare plans.

Communications that require authorization include "volunteer or community activities; pending state or federal legislation and joining grassroots advocacy organizations and information about such advocacy," the agency said.

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.

◆ **An Arkansas doctor and former employees are sentenced for HIPAA violations.** On Oct. 26, 2009, the Department of Justice and FBI announced the sentencing of Dr. Jay Holland, Sarah Elizabeth Miller and Candida Griffin. All three pleaded guilty on July 20, 2009, to violating HIPAA by accessing patients' protected health information without any legitimate purpose. At the time, Dr. Holland was the medical director at a hospital in Arkansas. He admitted to remotely accessing a patient's record out of curiosity after watching a news report about the patient. The hospital suspended him for two weeks and required him to complete online HIPAA training. Dr. Holland was sentenced to one year of probation, a \$5,000 fine to be paid in 60 days and 50 hours of community service educating professionals on HIPAA. Miller was an account representative at the same hospital in Arkansas as Dr. Holland. Miller admitted that on two separate days, she accessed a patient's record approximately 12 times out of curiosity and with no legitimate need to do so. Miller's employment with the hospital was terminated. She was sentenced to one year probation and a \$2,500 fine payable in installments. Griffin, who was the emergency room coordinator at the same hospital, also admitted to accessing a patient's record out of curiosity without any legitimate need to do so and was terminated from her position. Griffin was sentenced to one year probation and a \$1,500 fine payable in installments. The U.S. Attorney for the Eastern District of Arkansas stated: "We hope that today's sentencing send the message that the HIPAA protections apply to every person in the community, regardless of their position or stature. Likewise, the penalties for violat-

ing HIPAA apply equally to everyone with access to protected health information."

◆ **The Appellate Court of Illinois reinstated a patient's claims that a hospital improperly disclosed mental health records pursuant to a subpoena without a court order.** Kyoung Suk Kim filed an action alleging that St. Elizabeth's Hospital of the Hospital Sisters of the Third Order of St. Francis, the health system and its attorneys violated Illinois' Mental Health Confidentiality Act. Kim argued that St. Elizabeth's disclosure of her mental health records in a prior divorce proceeding pursuant to a subpoena that was not accompanied by a court order violated the Illinois law. The hospital argued that Kim had placed her emotional health, mental health and stability at issue in the divorce proceeding and that because the court in the divorce proceeding ruled that the records were relevant to the case, Kim was precluded from bringing the case against the hospital. According to the Appellate Court of Illinois, however, "the question of admissibility of Kim's mental health records, after they had been disclosed, is distinct from the question of whether the records were obtained by an improper procedure in the first place." The court went further to state that the court in the divorce proceeding did not determine that because Kim had put her mental health at issue, the defendants did not violate the Mental Health Confidentiality Act. Accordingly, the court reversed the dismissal of Kim's claims against the hospital for improperly disclosing her mental health records. (*Kim v. St. Elizabeth's Hospital, et. al.*)

In spelling out the procedure for obtaining and archiving authorizations, CMS notes that it is “adopting the same requirements for these authorizations as required by the HIPAA privacy rule.” “We are using the same approach that HIPAA requires to support uniformity,” Ashkenaz told *RPP*, noting that Medicare plans are also HIPAA covered entities.

So far, Humana is the only CE that has been publicly admonished for using PHI in this way. Blue Cross Blue Shield of North Carolina sent letters asking members to contact a U.S. senator to oppose a public option in national health reform, but a plan spokesman said it used voter records, not patient records, to select those who received the mailings.

Other CEs, including hospitals, have been involved in the health reform debate, but they have evidently been careful not to involve their patients. McGraw says she frankly was surprised by Humana’s action.

The American Hospital Association, for example, never asked its members to tap patients to contact Congress or express their thoughts on health reform. Instead, AHA worked directly with hospital executives, and held community forums in 2008 to solicit consumer input, said spokeswoman Alicia Mitchell.

CMS Action Plays to Mixed Reviews

McGraw says the fact that CMS found enrollment data were improperly accessed and the fact that it issued guidance emphasizing that enrollee signatures must be obtained should provide OCR with the foundation to prove the letters violated the privacy rule.

CMS’s statement to Humana “is the right way to interpret HIPAA, to be true to the intent of protecting patient privacy,” McGraw says. Humana and other CEs should use only PHI necessary for “the core of their business, which is delivery of and payment for health care,” she says.

But Jeff Drummond, a partner with the law firm of Jackson Walker LLP, based in Dallas, says Humana could defend the use of the enrollment data as falling into the category of “operations,” as it communicates benefits information to its members, he says, much like describing changes in a drug formulary. Using names and addresses, he says, surely qualifies as “minimal use,” and points out that while Humana used PHI for this purpose, it did not “disclose” any PHI.

He was angered by CMS’s attention to the issue, which he saw as hypocritical and “thuggish,” especially given that HHS itself has a link on its Web site that links to www.HealthReform.gov, and invites visitors to “state your support for health reform this year.”

“If HHS or Congress changed the Medicare Advantage program to allow coverage for a new procedure or

product, would the MA plan be prohibited from letting the beneficiaries know? No,” Drummond says. “If the Democrats’ health reform plan was going to add benefits to MA and the MA plans notified their beneficiaries about these possible new benefits, do you think in any way HHS would have started a HIPAA investigation? The answer to that question is pretty obvious.”

What Are Health Care ‘Operations’?

McGraw counters that “operations” has always been an undefined term that “has enough loopholes to drive a truck through.” Her organization and others unsuccessfully lobbied Congress to restrict use without an authorization to treatment (T) and payment (P) — and to leave out the O, or make it the subject of a study or project to define the term more clearly. This situation shows why that would have been a useful exercise, she says. “What isn’t under operations? Everything but selling you a timeshare? It borders on the ridiculous.”

Mark Rothstein, who for eight years was the highest ranking health care privacy advisor to the federal government, agreed that “operations” needs to be refined. “The term ‘health care operations’ has been construed extremely broadly. It is a key part of the privacy rule that needs to be reconsidered to limit the non-essential secondary use of protected health information,” says Rothstein, director of the Institute for Bioethics, Health Policy and Law at the University of Louisville School of Medicine. Until June 2008, he served as chairman of the privacy subcommittee of the National Committee on Vital and Health Statistics.

HIPAA expert Kirk Nahra, a partner with Washington, D.C.-based law firm Wiley Rein, LLP, tells *RPP* it is “not obvious” to him that the letters qualify as “operations” and he finds it to be a “close call.” Says Nahra: “I think it could fit somewhere, but it is not clearly within the scope [of operations].”

If OCR were to find that Humana did violate the rule, it has a variety of penalties at its disposal, including possibly requiring a corrective action plan and imposing fines, with penalties that were increased as a result of the HITECH Act (see story, p. 5).

OCR has collected payments from only two errant covered entities since the privacy rule went into effect in 2003, and it has been careful not to term as “penalties” the payments made by Providence Health and Services and CVS. But it pledged to step up enforcement as it absorbed security rule enforcement (*RPP* 9/09, p. 1).

Contact Ashkenaz at peter.ashkenaz@CMS.hhs.gov, Noland at tnoland@humana.com, McGraw at deven@cdt.org, Drummond at jdrummond@jw.com and Nahra at knahra@wileyrein.com. ♦

PRIVACY BRIEFS

◆ **House Energy and Commerce Committee Chairman Henry A. Waxman (D-Calif.) and Ways and Means Chairman Charles B. Rangel (D-N.Y.), along with several other ranking members of their committees, sent a letter to HHS Sec. Kathleen Sebelius urging her to repeal the “harm” standard in the HITECH Act breach notification rules.** Under the interim final regulations, released Aug. 24, covered entities are required to notify individuals of a breach when it poses a “significant risk of financial, reputational, or other harm to individuals” (*RPP 10/09, p. 1*). However, the letter notes, if the covered entity responsible for the breach determines that the breach did not pose harm, then “the provider or health insurer never has to notify their patients that their sensitive health information was used or disclosed in violation of the federal privacy rule.” The letter states that this “is not consistent with congressional intent.” See the letter at http://energycommerce.house.gov/Press_111/20091001/sebelius_letter.pdf.

◆ **The Tennessee Department of Health Services (DHS) unknowingly gave the wrong fax number to 100 medical providers statewide, causing them to send private patient health information to a businessman in Indiana,** *The Tennessean* recently reported. DHS says a new caseworker in the disability determination section sent out a cover sheet with a typo in the toll-free fax number. The state sent an e-mail blast to 29,000 providers with the correct contact information soon after the problem was found. Visit www.tennessean.com/article/20090929/NEWS01/909290346/2066/NEWS03/Tennessee+gave+doctors+wrong+fax+number+in+privacy+breach.

◆ **A portable computer storage device containing patient names and Social Security numbers went missing from Pitt County Memorial Hospital in North Carolina, according to an Oct. 14 article in the *Greenville Reflector*.** The hospital reported that the device was not located where an employee left it. Officials sent letters to more than 1,600 individuals whose information may have been compromised, offering a year of free credit monitoring and identity theft services. The hospital explained in the letters that it has taken precautions to prevent further breaches, including filing a police report, locking down portable devices, and educating employees. See the article at www.reflector.com/news/hospital-patient-info-is-missing-899251.html.

◆ **HHS published an online form for covered entities to use when reporting breaches of unsecured protected health information (PHI), as required under the HITECH Act.** According to the breach notification interim final rule, breaches of unsecured PHI involving 500 or more individuals must be reported to HHS at the same time they are reported to individuals, without unreasonable delay and within 60 days of discovery. A breach involving fewer than 500 people must be reported within 60 days of the end of the calendar year. The HHS form provides checklists for indicating the type of breach, location, type of PHI involved, and actions taken in response to the breach. CEs can submit the form electronically. Find the form at <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruc.html>.

◆ **A laptop containing approximately 850,000 physicians’ Social Security numbers and tax identification numbers was stolen from a Blue Cross and Blue Shield Association (BCBSA) employee’s car on Aug. 25.** The incident, which was announced by BCBSA in late-September, involved an employee who had proper access to the data but downloaded an unencrypted version of the information onto a personal laptop, in violation of BCBSA regulations. BCBSA is offering a year of free credit monitoring to affected providers. The breach doesn’t have HIPAA implications because the data did not contain protected health information, nor does it fall under the Federal Trade Commission’s breach regulations since there were no electronic health records involved.

◆ **The FTC announced on Oct. 30 it will once again extend the enforcement deadline for the identity theft Red Flags Rule, giving financial institutions and creditors until June 1, 2010, to address the issue.** The Red Flags Rule, instituted under the Fair and Accurate Credit Transactions Act, “requires all such entities that have ‘covered accounts’ to develop and implement written identity theft prevention programs to help identify, detect, and respond to patterns, practices, or specific activities — known as ‘red flags’ — that could indicate identity theft,” states the release. The commission decided to delay enforcement for a fourth time at the request of Congress, pushing it back from Nov. 1. See the press release at <http://www.ftc.gov/opa/2009/10/redflags.shtm>.

**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.)