Report on
PATIENT PRIVACY

Volume 10, Number 5 • May 2010

Practical News and Strategies for Complying With HIPAA

Contents

Go to www.AISHIPAA.com for subscriber-only access to 30+ narrative sections by privacy and security experts (including new content on the HITECH Act), back issues of RPP, *and much more. If you don't have a password, call 800-521-4323 or e-mail customerserv@aispub.com. Please whitelist aishipaa@aispub.com to ensure e-mail delivery of* RPP.

Déjà Vu 2003: Complicated 'Minimum Necessary' Rules May Be Baaaaaaack

With all of their new duties and responsibilities included in the HITECH Act, covered entities (CEs) and business associates (BAs) may have overlooked a provision requiring them, whenever possible, to clamp down on the release of information beyond the often misunderstood and inappropriately applied concept of "minimum necessary."

In a briefly worded provision, the HITECH Act required HHS to issue "guidance on what constitutes minimum necessary" within 18 months of passage, which would be Aug. 18, 2010. However, the law also said that until such guidance is issued and in effect, CEs and BAs should be sharing information through "limited data sets" — even when exchanged for treatment purposes.

Taken together, the requirement for guidance and the admonition to use limited data sets could portend a profound tightening up on the types of information CEs and BAs will be permitted to disclose and use in the future. Minimum necessary is a central tenet in privacy protections and comes into play thousands of times a day as CEs access and share protected health information with other CEs and business associates.

Another sign that things could change: The act also requires HHS to release guidance on methods to deidentify data, and it links the two tasks, saying that the minimum

continued on p. 10

Visitors to Facilities Take on Many Different Forms, but Present Similar Privacy Risks

When a blind therapist was hired by NHS Human Services, Inc., a large behavioral health care services provider, he requested the services of a helper to double-check the treatment records and other paperwork he fills out electronically. Because it was a "reasonable accommodation" under the Americans with Disabilities Act, NHS retained the services of the helper. Though not a member of the NHS workforce, the helper has access to protected health information, which means she is held to the same privacy-protection standards as NHS employees. The helper is required by NHS to submit to background checks and clearances required of employees, attend HIPAA and compliance training, and sign a confidentiality agreement, says Patricia Wynne, privacy officer and in-house counsel for Pennsylvania-based NHS. "The confidentiality agreement legally binds the helper to maintain the confidentiality of the PHI during the term of service," Wynne says. The confidentiality agreement also confirms that the PHI's protection survives the helper's services to NHS.

The helper is one example of the often-eclectic mix of outsiders who routinely cross the threshold of hospitals and other covered entities. The existence of a wide variety of outsiders requires an organized response by privacy officers to ensure the protection of patient privacy. Most health care organizations have pretty much nailed down ways to manage their HIPAA compliance in this area, although their approaches vary somewhat.

continued

There appear to be two different categories of outsiders who visit the facilities of covered entities:

(1) Those who have "actual or potential access to confidential information," who, according to Wynne, must be trained in HIPAA/HITECH and other compliance issues and/or sign confidentiality agreements. These outsiders usually aren't workforce members. They may be vendors or other business associates providing contractual services to the provider.

(2) Those who do not access PHI or, at most, have only incidental contact with providers (e.g., food or flower delivery people) and typically are not trained on HIPAA. However, policies and procedures must be in place to limit their access to critical service areas, Wynne says.

Even when outsiders are subject to business associate agreements, Wynne recommends on-going staff notices about maintaining confidentiality and/or getting signed confidentiality agreements from the individuals providing services (e.g., cleaning staff, interpreters, copier repairers, etc.) who enter service areas where there is potential access to PHI. The newly enacted HITECH Act has raised the stakes for business associates, which are now directly subject to HIPAA regulations and the penalties for noncompliance with the HIPAA and HITECH regulations.

Report on Patient Privacy (ISSN: 1539-6487) is published 12 times a year by Atlantic Information Services, Inc., 1100 17th Street, NW, Suite 300, Washington, D.C. 20036, 202-775-9008, www.AISHealth.com.

Editor, Liana Heitin; Contributing Editor, Nina Youngstrom; Executive Editor, Jill Brown; Publisher, Richard Biehl; Marketing Director, Donna Lawton; Fulfillment Manager, Gwen Arnold; Production Coordinator, Russell Roberts

Call Liana Heitin 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.

Three Categories of Visitors Identified

According to compliance and privacy director Frank Ruelas, Maryvale Hospital in Phoenix separates outsiders or visitors into three categories. They have "designated portals of entry" that manage their hospital assignments, which usually have a HIPAA interface, whether it's training or confidentiality attestations. The Maryvale categories of outsiders are:

◆ ***Residents who "shadow" community physicians and observe them in their hospital habitat:*** These are not residents in traditional teaching hospitals, he says. Some residents spend time training in physicians' practices to learn about different specialties. Part of this experience is observing the community physicians treating their patients in the hospital, which means they are exposed to PHI. They are not workforce members, however. The Maryvale Hospital portal for shadowing residents is the medical staff office, which makes sure the residents attend HIPAA training and sign confidentiality agreements in which they acknowledge they are bound by hospital policies and procedures. The residents attest they understand they will come into contact with patient information and will not use or disclose it.

◆ ***Deliveries***: These run the gamut, including people who deliver flowers to patients and office supplies to the hospital. Maryvale steers certain flower delivery people clear of patient-care areas and has them drop off their goodies to administration, with volunteers then bringing patients the flowers. "We try to centralize these folks," he notes. Office supplies and equipment are brought to materials management. But if supplies (e.g., water-cooler replacements) are heavy or unwieldy, the delivery person probably will get clearance to drop them off. Usually the delivery is intended for a common area anyway, Ruelas says. If delivery people have to go to a patient unit, materials management will escort them. "The chances the water guy will hear anything are slight," and anyway, it would just be an incidental disclosure, Ruelas notes.

◆ ***Vendors:*** Vendors are all over the map, but materials management is the Maryvale portal. "Vendors are anyone looking to sell us something or provide information about services," he says. For example, when post-acute care providers come to Maryvale to discuss referrals with the discharge planning department, they must go through materials management first. Every time they come into the hospital, vendors sign a sign-in sheet that

states they will safeguard the privacy and security of patient information. "The signature accomplishes the confidentiality pledge," he says.

Maryvale deals with other random outsiders individually as the need arises. Some are considered to be "insiders" (e.g., volunteers) and are treated as quasi-employees who are subject to HIPAA training.

HIPAA Permits Incidental Disclosures

According to the Office for Civil Rights, incidental disclosures are OK as long as the covered entity applies "reasonable and appropriate safeguards and implemented the minimum necessary standard, where appropriate." According to Neschla McCall, compliance director and chief privacy officer for Inova Health System in Fairfax, Va., the incidental disclosures provisions relieve CEs from the obligation to obtain confidentiality attestations from certain outsiders who have minimal exposure to patients, such as family members or friends of patients who are visiting. Random traces of PHI that such individuals may come into contact with are "incidental," and HIPAA does not require that all such risks be totally eliminated.

Because Inova has an affiliation with a medical school and a pharmacy school, students are frequent visitors to Inova's facilities. "They come here for their third and fourth years of training," McCall says. Their training programs fall under "health care operations," which means the students can use and disclose PHI without patients' authorizations for training purposes. According to OCR, "the definition of 'health care operations' in the privacy rule provides for conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers."

Inova treats medical and pharmacy students like quasi-workforce members. "We do HIPAA and compliance training and the physicians who are teaching them make them aware of the privacy rules," McCall says. They are trained on Inova's clinical information systems and receive IDs and passwords necessary to access patient information. "They can't make copies of PHI or disclose it outside of their training, and they get training on that," she says.

One group of outsiders that may be particularly troublesome is the cleaning crew. "We have always been concerned about janitors. They may have access to everything," says Harry Rhodes, director of practice leadership for the American Health Information Management Assn. "They come up as a possible risk during risk assessments."

A recent security breach drives home the potential vulnerability caused by cleaning crews, Rhodes says. In late March, a janitor allegedly stole information from up to 250 patients' files at a Northwestern University physician group in Chicago with the alleged help of relatives and friends, according to the Chicago Breaking News Center. The janitor, who apparently lifted files from unlocked cabinets, worked for a contracted janitorial service and was not an employee of the physicians' group, which is part of Northwestern Medical Faculty Foundation. The Cook County Sheriff's Department issued a felony arrest warrant for the janitor and her alleged conspirators, who were accused of using the patient information to obtain credit cards and go on shopping sprees, the sheriff told the news center.

Rhodes also urges covered entities to do a risk assessment when hiring building contractors. "Do an inventory of where your information is and identify potential vulnerabilities and threats. What are your security controls? Do they protect you from the contractor's inappropriate access? What information will be in the areas these guys are repairing? Is it possible the plumber will see or hear something he shouldn't? Are there unlocked file cabinets? Do you leave [PHI] on tables? Are computers up and running when you walk away?" If the privacy and security risks seem too great, Rhodes says, secure the information and keep it out of the contractor's sight, and/or consider asking the contractor to sign a confidentiality agreement.

Confidentiality Agreements Are a Good Practice

Vendors who enter a facility to update servers or work on copiers may have access to PHI and should sign a business associate agreement, Wynne says. "Also, if a company is hired to perform services for the provider and sends staff to perform data entry, billing, legal or accounting services, and the staff needs to access the provider's PHI in order to perform the services, a business associate agreement must be signed before access is given," she notes.

In situations where it's less likely the outsiders will have actual access to PHI, but they may be on site in critical service areas, it's a good practice to have such parties sign a confidentiality agreement. "NHS wants to make sure workers understand the need for privacy of PHI," Wynne says.

However, covered entities don't have to extend this to mail carriers or Fed Ex workers who drop off packages, Wynne says. The covered entities must have policies and procedures ensuring that these kinds of outsiders don't have access to critical areas of the service sites.

Christine Adams, privacy officer and compliance coordinator for Medical College of Georgia, the health sciences university of MCG Health in Augusta, Ga., developed a confidentiality agreement for the school of

dentistry candidates who are recruited and interviewed on campus. Because prospective students are exposed to PHI during their tours, she says, it made sense to develop a statement they can sign to pledge their commitment to patient privacy. The theme of the attestation, which Adams adapted from one used at Vanderbilt University, is "what goes on in the dental school stays in the dental school," she says. Before touring, potential students must sign a statement that says, in part:

> "You may see or hear information related to MCG patients (such as charts and other paper and electronic records, demographic information, conversations, admission/discharge dates, names of attending physicians, patient financial information, etc.). Any patient information you see or hear, either incidentally or by attending rounds, must be kept confidential. By signing below, you are agreeing to abide by MCG policies regarding confidentiality of patient health information."

Contact Wynne at pwynne@nhsonline.org, McCall at neschla.mccall@inova.org, Ruelas at frank@hipaabootcamp.com and Rhodes at harry.rhodes@ahima.org. ✧

1974 Privacy Act Has Led to Bias in OCR's Posting of Security Breaches

Some covered entities, such as Sands Hospital at the University of Florida and Cardiology Consultants/Baptist Health Care Corporation, have seen their names in big type on the federal government's privacy and security breach "wall of shame."

But a handful of unidentified HIPAA transgressors, who also experienced a breach of protected health information of more than 500 patients, has been listed simply as "private practice," with just their city and state.

By summer, that will change, and those CEs that have heretofore been cloaked in mystery will be identified. The Office for Civil Rights, which maintains the breach list on a website (http://tinyurl.com/yczfmgy), intends to adopt a policy allowing it to identify the practices by name, and it will apply the change retroactively, *RPP* has learned.

Yet at least one health care attorney says listing any names is a bad move. Kirk Nahra, who calls the listing "unnecessarily punitive," says CEs involved in "close cases" that might not demand reporting should weigh whether they should remain mum to avoid being placed on the OCR list. Having the list provides CEs with a "disincentive" to report, he maintains.

Advocates Hailed New Reporting Rules

When Congress passed the HITECH Act, privacy advocates immediately hailed a provision they said would help strengthen protections for patients, namely the requirement that any breach affecting 500 or more individuals be reported to the news media and to OCR, for it to post on a public website. A breach of any size is also to be reported to affected individuals and to OCR in an annual report *(RPP 9/09, p. 1)*.

A year after the law was signed, OCR posted the first list of these breaches *(RPP 3/10, p 1)*. In all but a handful of cases, OCR identified the responsible covered entity by name, and the business associate, if applicable. As with the identified CEs, the unidentified entities were listed with the number of affected individuals, the date and type of breach and the location of the lost protected health information...yet their names remained a secret.

On Feb. 20, for example, a practice in San Antonio experienced a theft of a portable electronic device affecting 21,000 people. A similar theft in December at a private practice in Stoughton, Mass., exposed the medical records of some 1,800 patients.

While some debate the value of listing the names, many are puzzled by the anonymity accorded to some CEs, saying it seems unfair. In an April 13 *Federal Register* notice, OCR, for the first time, explained its actions. Technically, it issued a "notice of modified or altered system of records."

OCR's contention is that the federal Privacy Act of 1974 "prohibits OCR from publishing the name of a covered entity that is an individual and not an organization or institution without an appropriate routine use in place or without their permission," which is why it published the System of Records Notice (SORN), William Hall, an HHS spokesperson, tells *RPP*.

"Because of the Privacy Act of 1974 limitations, OCR responded by issuing a SORN to modify our existing system of records to incorporate the new information collection on breaches required by the HITECH Act and to expand the routine uses for this new information collection to include the purposes under the HITECH Act for the collection of this information," Hall says.

The notice did not appear to address whether the naming would apply to those currently on the list, but Hall confirms it will.

"OCR intends to apply the new routine use retroactively, so the names of all covered entities currently listed as 'private practice' will be published" once the change goes through, he says.

The comment period ends May 23. Following that, "OCR anticipates beginning to publish the names of covered entities currently listed as 'private practice' some time after that." Breaches go through a bit of a screening process before they are posted. Anyone can report a breach, so OCR checks with the entity.

"When OCR receives a report of a 500-plus breach, the OCR regional office contacts the covered entity to confirm that the information is accurate before the information is posted on the website," Hall says. "Currently, if the name of the covered entity is an individual and not an organization or institution, OCR cannot publish the name of the covered entity."

Believing it did not have the authority to post these names, OCR has been asking private practices if they would consent to be named.

Although OCR is seeking comments on the naming issue, it would appear it is firm in its plans. It may receive feedback from CEs that don't wish to be named and oppose the proposed change. Others tell *RPP* OCR has the authority to be naming everyone now, and they aren't buying the Privacy Act reasoning.

'There Is No Reason Not to Name Them'

"I just don't see any reason not to name them," Jeff Drummond, partner in the law firm of Jackson Walker LLP, based in Dallas, tells *RPP*. "The Privacy Act defense just depends on what the 'purpose' of the disclosure to HHS is in the first place, so that he or she can take steps to prevent damage. If the notification requirement were to help the affected individuals, then it seems that they would need to know *who* disclosed the info. So, publicly disclosing the names of the CE would be a purpose of the provision of the information to HHS in the first place, and would not violate the Privacy Act."

Likewise, "if the requirement to notify HHS is for punishing CEs, then the names of the CEs could be disclosed without violating the Privacy Act," he adds.

Those entities that are now going to be named might not like it, but Drummond, former OCR director Rick Campanelli, and others say the change makes sense.

"I think OCR is just aligning their practice with what most people anticipated would occur as a result of the HITECH Act…that covered entities and business associates that have to report breaches — private practitioner or not — under the HITECH Act likely expected that their reports would become public," he says.

Campanelli, a partner in the Washington, D.C., law office of Baker & Daniels LLP, welcomes the new identification policy. "I support the change because I don't think it makes a lot of sense to differentiate who will be identified on the basis of size, when a significant breach occurs."

Since the list is just a few months old, it is too soon to tell what impact it might be having — either on compliance or the reputation of CEs. But Campanelli thinks it can serve as a deterrent to other CEs.

"Being identified certainly adds to the incentive to be more careful about having a breach occur in the first place. Of course, the HITECH breach notification requirements, including the obligation to mitigate, are themselves significant incentive to avoid breaches," Campanelli says.

Some May Be Swayed Against Reporting

But Nahra, a partner in the Washington, D.C., law office of Wiley Rein LLP, fears an opposite effect.

"I can agree with the criticism" about leaving off the names, he says. "I don't see why one category would be treated any differently. But I personally don't like the whole posting [requirement] and the media notification." The purpose of notifying individuals is so they can take steps to prevent damage from exposure, he notes. Once that's done, isn't it enough? he asks.

CEs don't legally have to notify OCR or patients unless the loss or inappropriate disclosure of PHI is a real breach and poses a "significant risk of harm" *(RRP 10/09, p. 1)*.

The assessment about whether the situation poses a "significant risk of harm" isn't always clear-cut, and when the CE ponders whether to report when it really doesn't have to, it should weigh the impact of any adverse publicity that is likely to result from OCR's listing, Nahra says.

Instead of the list, OCR should try to analyze patterns in the breaches and provide guidance on how to prevent them, he says.

"I think HHS could do something helpful; they could look at all these breaches and say, 'There is a problem with XYZ, and there are things you can do,'" and list them, Nahra says. "I am not sure there is any additional value to the mere publicity of just listing people."

Contact Nahra at KNahra@wileyrein.com, Hall at bill.hall@hhs.gov, Drummond at jdrummond@jw.com and Campanelli at Richard.campanelli@bakerd.com. ✧

CEs Encrypt Data Selectively Despite an 'Implicit Mandate'

A search for "encryption" — or any form of the word "encrypt," for that matter — within the HITECH Act turns up zero results. But privacy experts say there's an implicit mandate for encryption in the HIPAA security rule now that the technology is accessible and affordable.

Experts on the technical side see a nuance — while encrypting data in motion is a must because of their vulnerability to breaches, encrypting data at rest, such as electronic medical records (EMRs), can impair performance and may not be worth the cost.

Covered entities and business associates that do not encrypt PHI and experience a breach are vulnerable under the new security breach notification obligations *(RPP 9/09, p. 1),* says privacy and security compliance expert Chris Apgar.

When the HIPAA security rule was published in 2003, encryption was "addressable" rather than required, Apgar explains. An addressable specification must either be implemented or have documentation about why it is not reasonable or appropriate to implement and an equivalent measure must be used in its place. In 2003, "encryption was expensive, not considered mature or ready to use, and not necessarily interoperable.…[It was] burdensome from an administration perspective," says Apgar, president of Portland-based Apgar & Associates.

'No Excuse' Left for Not Encrypting

However, seven years later that's no longer the case. Organizations have "no excuse" for not using the technology these days, Apgar says, since even a two-person physician practice can implement e-mail encryption for $100 a year (see box, p. 7).

Encryption is "an *ad hoc* standard," says John Parmigiani, a HIPAA compliance expert who helped author the federal security rule. "Though they haven't officially mandated it, you'd better have a pretty good reason why you didn't do it." The encryption must meet the National Institute of Standards and Technology (NIST) thresholds (http://csrc.nist.gov/publications/PubsSPs.html) in order to comply.

Parmigiani, president of John Parmigiani & Associates, LLC in Maryland, points out that the April 2009 HHS guidance for the breach notification rule states there are only two ways to render PHI secure: encryption and destruction *(RPP 5/09, p. 11)*. CEs and BAs that encrypt data avoid the breach notice requirement and, in effect, have a safe harbor, says Parmigiani. "Again, without saying you have to do this, they're saying if you don't do it, you're opening yourself up for potential grief and time and money," says Parmigiani.

And the monetary stakes for failure to encrypt are now higher than ever. The HITECH Act amended HIPAA to ramp up monetary penalties for violations, pushing the maximum penalty to $1.5 million. The new fines apply to violations that occur on or after Feb. 18, 2009.

Data in Motion Should Be Primary Target

There's no doubt organizations should be encrypting data in motion, says Paul Fowler, vice president of Healthcare Innovation for Phoenix, Ariz.-based Axway, a software company that facilitates business interactions. That includes PHI sent through e-mails and physically transported on laptops and thumb drives — all of which are vulnerable to theft or interception. (Though the HHS interim final breach notification rule states that thumb drives should use the "data at rest" NIST encryption standards, it is most helpful to think of any transportable data as "in motion.") Organizations that are not encrypting data in motion "don't have a true awareness of the risk," says Fowler.

The HHS Office for Civil Rights is now posting on its website a list of CEs and BAs that have experienced breaches of unsecured PHI affecting 500 or more individuals (see story, p. 4). So far, the most common causes of breaches are lost or stolen laptops with PHI that were not encrypted.

More and more providers are finding ways to encrypt moving data and avoid the harsh new penalties. "E-mail encryption is a massively growing business," Fowler says.

According to the Healthcare Information and Management Systems Society (HIMSS) Security Survey, released November 2009, 67% of responding information technology executives said they encrypt data in transmission, with 60% encrypting e-mail and 39% encrypting mobile devices. E-mail encryption and single sign-on were identified most frequently as technologies that were not yet installed but planned for future installation *(RPP 12/09, p. 6)*.

Yet when it comes to data at rest, many organizations are opting to conserve their resources. Ruby Raley, director of health care solutions for Axway, says "I don't know of anyone who is encrypting electronic medical records," noting that she works mainly with large enterprises.

Think of a hospital as a fortress, Raley says. "Deep in the heart of the fortress you're less likely to be attacked directly. You're more likely to be attacked when moving outside the perimeter. There are lots of things

you need to do to secure the perimeter before worrying about the EMR database itself."

The HIMSS Security Survey found that 44% of respondents encrypt stored data and 39% use network encryption.

There are two key reasons cited for not encrypting data at rest, says Fowler. First, encryption can hinder performance. A physician who is constantly un-encrypting and re-encrypting medical records loses a lot of time that could be spent with patients. Parmigiani explains that many hospitals and offices have legacy computer systems that are either not capable of handling encryption at all or the technology slows the system down considerably. "What if someone has a

How to Navigate the Maze of Encryption Products

While experts may disagree on whether protected health information stored on an internal network needs to be encrypted, it's clear that all health care organizations should at a minimum be encrypting their data in motion. HHS has pushed this point by giving covered entities and business associates a safe harbor from the breach notification obligations if they encrypt their PHI. And though the growing encryption market can be confusing, factors such as the intended number of users, the sophistication of the technology needed and cost should all help narrow down a covered entity's options when shopping for encryption products.

The cheapest products — read: "free" — are open-source encryption programs, which are in the public domain and have source codes that are visible to anyone. Proponents of open source cryptography say it is more secure because it can be examined and verified by a community of experts. Flaws and security holes can be found and fixed right away.

Andrew Lewman, executive director of Massachusetts-based The Tor Project, a nonprofit organization working to protect online privacy, recommends TrueCrypt, which he claims is "well-used and well-tested." With TrueCrypt, the user needs a password or a key, such as a USB drive with a favorite song or other personal file, in order to gain access. Unfortunately, as is the case with many encryption products, if the password or key is lost, there is no mechanism for recovery.

And while the open-source technology itself is free, its implementation may not be. Lewman says security programs, open source or not, "require a fairly advanced administrator to implement them correctly. That person could be worth $100,000 year, but that may still be cheaper than buying other products." There are also costs associated with staff education and training for any new product.

Open source "makes sense" for a small single-provider office, says Chris Apgar, president of Portland-based Apgar & Associates, "as long as you make sure it meets the requirement for appropriately encrypting information and is a secure product." He notes that the technology should match or exceed the National Institute of Standards and Technology encryption standards (http://csrc.nist.gov/publications/PubsSPs.html).

Apgar, who leans toward vendor products rather than open source, is quick to recommend DataMotion for e-mail encryption, a company he has used for the last seven years. Monica Hutton, the marketing director for DataMotion, explains that the company secures only data that are in transit (hence the name) and has products for offices and hospitals of all sizes and encryption needs. The small and medium-sized clients are "typically interested in the compliance piece of securing e-mail." They might use an application service provider (ASP) model, in which users log in to a secure website to compose, send and receive e-mail. The receiver gets a Web link and can compose a response, which can include attachments, and send it from the secure website as well.

Larger entities tend to want their own secure e-mail platform that allows them to transfer large files and send secure e-mail directly through their Outlook server. "We also have a policy engine for organizations that don't want the user to have to know whether to send an e-mail securely" or are trying to step up their e-mail security procedures, Hutton says. The engine "scans e-mail for data that should be sent securely, and if it determines it needs to be sent securely it automatically encrypts."

Hutton would not discuss pricing details, but Apgar says it costs about $100 per individual per year for the ASP model, and approximately $10,000 or more for the application and hardware appliance that plugs into the Microsoft Outlook server.

ZL Technologies, Inc. is another company that offers products for organizations of different sizes. It

continued

super duper encrypted algorithm and you can't open it?" These concerns are "legitimate," he says.

Second, according to Fowler, hospitals and other covered entities have their own secure networks, which they see as sufficient for internal communications. "I personally believe it, and wouldn't be concerned," he says. A virtual private network works as well as encryption in some cases, he says — for instance, an employee can dial in remotely rather than put encrypted information on a laptop.

Parmigiani says this reasoning is specious. "Some say they don't need encryption because they have a firewall. But that's just one of safeguard, one barrier," he says. "If you have a moat around your house, OK, but what if they get across the moat? Is it OK they're in?"

How to Navigate the Maze of Encryption Products (continued)

began as a secure e-mail vendor a dozen years ago under the name ZipLip, and has now added secure electronic archiving to its repertoire. Steve Chan, the vice president of business development, explains that the company utilizes both "push" and "pull" e-mail encryption methods, meaning the secure message is either pushed to the user's inbox or the user is pulled to a secure portal.

The ZL encryption software is "designed for high volume," says Chan, so most of the company's clients are large entities such as hospitals and pharmacies. Like DataMotion, ZL has the capability to scan e-mail for PHI and encrypt automatically if necessary. The cost depends on the number of users and the sophistication of the technology needed, but the base price is $15,000, Chan says. "For a small entity that may be a lot…but that provides full breadth of functionality" and is most often purchased by large companies. According to Chan, Walgreens has been one of ZL's customers for the last seven years.

Apgar also suggests health care organizations look into Sigaba, a company that secures data in motion and is geared toward medium to large organizations, and Cisco, which provides a host of security products and is tailored to larger entities. He says Tumbleweed, which merged with Axway in 2008, is "the Cadillac — but they won't talk to you for less than $150,000."

Beware of Encryption 'Snake Oil'

Pretty Good Privacy (PGP) Whole Disk Encryption is another good option, says Lewman. The product encrypts hard drives on laptops, desktops and removable devices and retails for $149, according to the PGP website.

When considering encryption products, says Lewman, it's critical to make sure they are peer-reviewed and use only published algorithms. "You want ones that have been through rigorous review. Watch out for companies that say, 'We developed this new, secret algorithm, and we can't tell you how it works because someone will break it.' This is the equivalent of snake oil."

He also notes that "no [product] has a risk of zero — and that's based on humans. The math may be flawless, but the implementation may have some flaws," which can leave the data open to attack.

Chris Walker, information security advisor to Internews Network, an international media development organization, offers a caveat for consumers of encryption products: "Remember that sacrificing usability for 'security' frequently backfires by creating incentives for people to resist the adoption of new tools and bypass new policies." For instance, he says, if a user is forced to generate a new password every one or two weeks, he might write it on a Post-it note and tack it up in his cubicle. "Or [imagine] an awkward-but-secure internal e-mail system that sits idle while everyone in the office uses their Gmail accounts to communicate with one another."

Walker says that when seeking out encryption technology, consumers should be looking for "a specific product that is (a) extensively-reviewed by security researchers, (b) widely-deployed within the health care sector and (c) well-respected by both…existing consumers as well as independent security professionals."

Contact Apgar at (503) 977-9432 or capgar@apgarandassoc.com, Lewman at (781) 424-9877 or andrew@torproject.org, Hutton at (973) 455-1245 or monicah@datamotioncorp.com, Chan through Rob Elliott at (408) 240-8989 or relliott@zlti.com and Walker at cwalker@internews.org.

RPP *subscribers should contact editor Liana Heitin (at lheitin@aispub.com) to share their experiences with different encryption products. Please comment on pros, cons, costs and other noteworthy features, and indicate whether your comments are OK to publish or off-the-record.*

Of course budget concerns are also fueling providers' decisions regarding encryption, says Raley. "Hospitals don't have tons of money. It's costing so much to implement electronic medical records — it's really expensive." And with many new regulations to comply with, choosing how to dole out funds is a matter of "triage," she says. Providers need to tackle their biggest risks first, which for most are their business associate agreements.

Raley also says that "if you start encrypting all outbound data, you'll start protecting data at rest." Fowler furthers the point, saying eventually "all that's left open is the rare probability of someone walking in and physically stealing a database."

But … an Entire Database Could Be Stolen

But unfortunately that can happen. In October 2009, a thief walked away from a BlueCross BlueShield of Tennessee training facility with 57 unencrypted hard drives containing 1 million members' data *(RPP 12/09, p. 12).* The hard drives were small — 3½ by 10 inches — but they were sitting in a storage closet, not in transport. Perhaps they should have been treated as data in motion since they were portable. Even so, the OCR breach list has several instances of desktop computers being stolen as well.

Privacy and security experts do agree that there's no security magic bullet. An organization that encrypts both data at rest and in motion is still subject to data leaks by authorized employees who decide to snoop. But as Apgar sees it, encryption is an "insurance policy" because it offers a safe harbor.

Fowler says that protecting data in motion is "relatively inexpensive" and should be a priority so that medical data can be shared more easily and patient care improved. But data at rest, he says, can be protected in traditional ways. "Realistically, you should do everything you can to protect systems inside without killing performance, and do everything you can with data in motion, including encryption," he says.

Contact Apgar at (503) 977-9432 or capgar@apgarandassoc.com, Parmigiani at (410) 750-2497 or jcparmigiani@comcast.net, and Fowler and Raley through Jennifer Usher at (415) 591-8456 or jusher@shiftcomm.com. ✧

PATIENT PRIVACY COURT CASES

This monthly column is written by Kayla Tabela 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 Tabela at ktabela@sonnenschein.com.*

◆ **A Tennessee court found that a physician's letter disclosing protected health information (PHI) is permissible under HIPAA.** On March 11, the Tennessee Court of Appeals ruled that a physician's disclosure of PHI did not violate the privacy provisions of HIPAA. In her complaint, Teresa Gard alleged false light invasion of privacy and defamation resulting from a letter sent by Dennis Harris, M.D., to other health care professionals involved in Gard's treatment. Harris was treating Gard in connection with a worker's compensation claim. After viewing a surveillance video of Gard performing various activities with significantly less pain than she exhibited in his office, Harris informed Gard that he would no longer provide her with medical care. Harris documented his decision in a letter to Gard, and sent copies of the letter to the physician who referred Gard to Harris, Gard's worker's compensation case manager and the case management company. In his letter, Harris also suggested future treatment options and recommended that Gard stop using narcotic prescription drugs. Gard contended that the letter contained false and defamatory statements, and that Harris' disclosure of this information violated her right to confidentiality. Specifically, Gard asserted that (1) the letter was not a medical record within the purview of HIPAA, and (2) the consent form she signed permitting Harris to use and disclose her PHI to "carry out treatment, payment, and health care operations" was too vague to waive her right to confidentiality. The court, however, disagreed. It found that Harris' letter fell within the meaning of "treatment," as defined by HIPAA, because it stated how Gard should proceed with finding health care services for her needs. The court also found that Harris' disclosure of PHI to other health care professionals was within the scope of Gard's consent because the individuals to whom Harris disclosed were connected to the management of Gard's health care or to her worker's compensation case. Put differently, Harris' disclosure of Gard's PHI was permissible under HIPAA because the disclosure was for the purpose of Gard's treatment. *(Gard v. Harris)*

Minimum Necessary Could Heat Up

continued from p. 1

necessary guidance "shall take into consideration" the deidentification guidance.

The Office for Civil Rights, which will write both guidances, is behind schedule in releasing regulations and guidance implementing some of the provisions in the HITECH Act. However, it recently held a two-day meeting on the deidentification issue to solicit feedback from security and technology experts about the ways that data can remain safe and private. (For more information, see www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/deidentificationworkshop2010.html.)

'Minimum Necessary' Was Always Unclear

The original privacy rule, as OCR notes, "generally requires covered entities to take reasonable steps to limit the use or disclosure of, and requests for, protected health information to the minimum necessary to accomplish the intended purpose." It applies to payment and health care operations, but not to some treatment purposes. There has always been confusion about treatment, and OCR did little to clear this up when it deviated from the standard lingo of "uses" and "disclosures" in its description of how the minimum necessary concept is to be used regarding treatment.

According to OCR, minimum necessary "does not apply" to "disclosures to or requests by a health care provider for treatment purposes." Note it does not say "uses" but instead says "disclosures" and "requests." But OCR has confirmed to *RPP* that minimum necessary does, in fact, apply to the uses of PHI for treatment purposes.

Further complicating a CE's understanding was that OCR *did* use the phrase "uses and disclosures" in describing another exception, when it said that minimum necessary does not apply to "uses or disclosures made pursuant to an individual's authorization."

It can be instructive to review congressional intent behind concepts that are included in laws and then are passed on to private entities through government regulations. If the regulation (or, in some cases, even guidance) deviates from the intent, members of Congress sometimes go back to an agency and demand changes. One example of this is underway now, with some members having objected to OCR inserting a new "harm" standard in the rule implementing the breach notification requirement *(RPP 11/09, p. 12)*.

It is not known where the idea of guidance or limited data sets came from. But it does reflect the findings of an $11.5 million, two-year study released in 2007, which recommended that a federal standard for minimum necessary be developed — or that it be scrapped altogether — because there was so much documented misapplication of the concept *(RPP 5/07, p. 3)*.

The study, although designed to show gaps that might make a national health information network difficult, marked the first (and, so far, the only) large-scale look at compliance across the U.S. Researchers analyzed privacy and security compliance in Puerto Rico and 33 states that together make up the Health Information Security and Privacy Collaboration.

Conducted by Research Triangle International, the study found that many organizations were applying minimum necessary to treatment, with some even applying it in-house; some thought it was OK to apply it to "uses" since that word was omitted.

Linda Dimitropoulos, senior director of RTI's health services research program, tells *RPP* she was pleased to see that Congress had acted on the recommendation for clarity, and says the need still remains today.

"We were really happy to see that," Dimitropoulos says, adding that RTI was not consulted as the HITECH Act was being drafted. "We found that there was not only tremendous variation in how organizations defined 'minimum necessary' but also much confusion about how to apply it. That continues to exist today," Dimitropoulos says. "I think guidance will go a long way toward standardization, although it will be a challenge" to draft.

What Should CEs Do Now?

Covered entities contacted by *RPP* were mostly unaware of the limited data set provision in the HITECH Act, and were vaguely knowledgeable about impending guidance related to minimum necessary. They also acknowledged that they were, in many cases, applying the minimum necessary concept to treatment-related exchanges of PHI.

With so many other new requirements to address, many covered entities are simply awaiting the guidance and said they intended to make changes as needed once it was released.

But this may not be totally consistent with what the law says. And with strong signals that deidentification requirements are likely to play a central role in the expected guidance, Dimitropoulos and other privacy experts are recommending that CEs take steps now to prepare for changes. While it might be difficult to try and use only limited data sets, they should at least gain experience with what this concept means.

In addition, they should be reviewing their current minimum necessary policies to see how broad they are and how they might be applied more narrowly.

"I think [the requirement for guidance] signals that officials should be tightening up" their uses and disclosures policies, Dimitropoulos says. The law itself, in mentioning limited data sets, "was sort of a bit of guidance…. If you are going to make a decision, err on the side of a limited data set."

"We can't predict how restrictive the [guidance] will be, but I don't think it will go the other way," she says. Dimitropoulos suggests that CEs and BAs "take a good look at their existing policies and see what identifiers are really necessary. That is not a bad idea in preparation for whatever comes out."

Data Set Concept Was Surprise in HITECH Act

A limited data set is a concept in use since the privacy rule was published in 2003 but previously applied only to disclosures for research, public health and some health care operations. The appearance of this in the HITECH Act was surprising.

Specifically, the act states, "a covered entity shall be treated as being in compliance with [HIPAA with] respect to the use, disclosure, or request of protected health information described in such section, only if the covered entity limits such protected health information, to the extent practicable, to the limited data set…or, if needed by such entity, to the minimum necessary to accomplish the intended purpose of such use, disclosure, or request, respectively."

To qualify as a limited data set, the following identifiers must *not* be present:

(1) Names,

(2) Postal address information, other than town or city, state, and ZIP code,

(3) Telephone numbers,

(4) Fax numbers,

(5) E-mail addresses,

(6) Social Security numbers,

(7) Medical record numbers,

(8) Health plan beneficiary numbers,

(9) Account numbers,

(10) Certificate or license numbers,

(11) Vehicle identifiers and license plate numbers,

(12) Device identifiers and serial numbers,

(13) URLs,

(14) IP addresses,

(15) Biometric identifiers, and

(16) Full-face photographs and any comparable images.

When asked by *RPP* for any information on what the guidance might contain, OCR confirmed it was "currently developing guidance regarding minimum necessary and cannot comment further on this activity."

In ordering the minimum necessary guidance, Congress acknowledged that it did not want to impede clinical care or research, stating that HHS should also consider "the information necessary to improve patient outcomes and to detect, prevent and manage chronic disease."

OCR may not have an easy time drafting the guidance, Dimitropoulos points out. Any guidance that is "too restrictive" will be a problem, and she expects OCR ultimately "will still allow quite a bit of latitude."

"Those who are going to be asking for access to health information have to really put forward a clear rationale for why they need the data," Dimitropoulos says. "We do need to know more about what's necessary and what isn't. It doesn't take too much to reidentify data." She says the medical establishment's thinking about how data can be reidentified has become quite sophisticated.

Deven McGraw, a leading privacy advocate who serves on a government information technology advisory committee, tells *RPP* she will be looking for OCR to clamp down on exchanges of information for operations and payment, but believes information must be free-flowing for treatment purposes.

Limited Data Set Not Useful in All Cases

A limited data set may be useful as a default definition for PHI used in public health and research, "but it will not be useful for all that minimum necessary applies to," adds McGraw, the director of the Health Privacy Project at the Center for Democracy and Technology.

She calls the congressional intent "laudable," with the idea being "getting people thinking about identifiability of the data rather than the amount of data" when they consider what minimum necessary means.

McGraw says the mention of limited data sets should "send a message to OCR that they should be focusing on data deidentification."

The idea, she says, is to "create types of data sets that people use for routine purposes" that have some identifiable data removed. The guidance, in her view, should "offer some additional data options, along with limited data sets… [and] options for how to remove identifiers from the data and still have it be useable."

"If [the guidance] offered options on data masking and the stripping of identifiers, that would be landmark," McGraw says. She notes that, for example, data sent for use in quality reviews or for credentialing physicians need not contain personal identifiers.

Contact McGraw at deven@cdt.org. ✧

PRIVACY BRIEFS

◆ **A laptop with demographic and health information for 3,526 patients of the Massachusetts Eye and Ear Infirmary was stolen from a physician who was lecturing in South Korea**, according to the Boston-based hospital's April 20 statement. The laptop belonged to Robert Levine, M.D., a neurologist, and contained information — including names, addresses, phone numbers, dates of service, medical record numbers and test results — about patients he treated between Feb. 3, 1988, and Feb. 16, 2010. The laptop, which was stolen Feb. 19, was password-protected and had a tracking device known as LoJack. The device sent an alert on March 9 when the stolen computer was connected to the internet in South Korea. The hospital is offering affected individuals one free year of credit monitoring and other services. Go to www.masseyeandear.org.

◆ **Boulder Community Hospital (BCH), in Boulder, Colo., announced last month that several of its patients were mailed copies of their protected health information by an anonymous source who claimed it had been stolen from recycling storage bins**. The hospital says it is investigating when the theft occurred and has reported the incident to the HHS Office for Civil Rights. Hospital employees are now using self-locking storage bins and doing spot checks of the recycling system, the hospital states. Patients who become victims of identity theft as a result of the incident will not incur financial loss, according to BCH. See the press release at http://tinyurl.com/38ct7jz.

◆ **George Washington University, under contract with the Office of the National Coordinator for Health IT (ONC), issued a white paper examining how much control individuals should have over their health information in an electronic health information exchange.** "Consumer Consent Options for Electronic Health Information Exchange: Policy Considerations and Analysis" details the range of consent models for electronic exchange — which include no consent, opt-out, opt-out with exceptions, opt-in and opt-in with restrictions — and the challenges associated with selecting and applying a model. The white paper will serve as input to the HIT Policy Committee's Privacy and Security Workgroup. Read the white paper at http://tinyurl.com/ydedcpp.

◆ **A biannual HIMSS Analytics survey found that health care organizations are becoming more aware about patient data security but have not implemented "comprehensive and sustainable changes" needed to improve the handling of protected health information**. The *2010 HIMSS Analytics Report: Security of Patient Data*, commissioned by Kroll Fraud Solutions and released April 5, states that hospitals are focusing on how to handle a breach after it has occurred rather than focusing on risk assessments. It also says many organizations are not aware of the high costs associated with a breach as a result of the HITECH Act. The study found problems with the auditing of third-party vendors — only 60% of respondents required third-party vendors to provide proof of employee training, and 50% required their third-party vendors to provide proof of employee background checks. Find the report at www.krollfraudsolutions.com.

◆ **Blue Cross & Blue Shield of Rhode Island (BCBSRI) announced April 16 it had inadvertently given away a filing cabinet containing personal information for 12,000 of its Medicare members**. The insurer donated the cabinet to a nonprofit before removing Medicare health surveys from 2001 to 2004, which included members' names, addresses, telephone numbers, Social Security numbers, Medicare identification numbers and self-reported medical information. BCBSRI says it has notified federal and state authorities and sent letters to affected individuals. The insurer is offering affected members one year of free credit monitoring. According to BCBSRI's statement, the responsible employees have been disciplined, and several have been terminated, as a result of the disclosure. See the company's statement at www.bcbsri.com.

◆ **The South Carolina Department of Health and Environmental Control (DHEC) has notified 3,000 clients that their personal information may have been exposed after documents were improperly discarded in a recycling container.** According to the April 23 DHEC statement, the documents included patient information submitted to DHEC between Jan. 8 and Feb. 17, 2010, to determine eligibility for payment by agency programs to private health care providers. Some documents contained such detailed information as Social Security numbers, medical histories and test results. A third party found the documents in a bin behind the DHEC building and gave them to another individual, who returned them to DHEC. The agency sent letters to 1,800 individuals whose records were returned as well as all other individuals whose records were submitted during that time period. The information does not appear to have been used for criminal purposes, says DHEC. See the DHEC statement at www.scdhec.gov.

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.)