Report on
Patient Privacy

Volume 16, Number 6 • June 2016

Practical News and Strategies for Complying With HIPAA

Contents

Editor
Theresa Defino
tdefino@aishealth.com

Associate Editor
Lauren Clason

Executive Editor
Jill Brown

Compliance With New Gender Bias Rule Requires Focus on Patient Access, Privacy

Perhaps the easiest way to understand the privacy implications of the new 200-plus-page final rule issued by HHS's Office for Civil Rights (OCR), which prohibits gender discrimination in health care programs, is to consider this: Not every patient is like Caitlyn Jenner, the former Olympic athlete Bruce Jenner who had little to fear from publicly chronicling her transition to a woman.

Nearly three years in the making, the final rule implements Section 1557 of the Affordable Care Act (ACA), which bans discrimination on the basis of gender identity, alongside traditional prohibitions regarding race, color, religion, national origin, sex, disability and age. It "requires that women be treated equally with men in the health care they receive and also prohibits the denial of health care or health coverage based on an individual's sex, including discrimination based on pregnancy, gender identity, and sex stereotyping."

The final rule — which has major implications for HIPAA covered entities (CEs) — also "requires covered health programs and activities to treat individuals consistent with their gender identity," a fact sheet explains.

A hospital, doctor's office or other CE could unwittingly violate the law (and now the regulation) if steps are not taken now, says Dru Levasseur, director of the Transgender Rights Project for Lambda Legal.

At a minimum, CEs will need to ensure, and revise as necessary, their admitting and rooming policies to comply with the regulation, and those that provide health insurance may also need to redesign their plan benefits.

continued on p. 9

With Office for Civil Rights Audits Starting, It's Time to Panic, Maybe Just a Little

Covered entities (CEs) around the country have been getting lots of emails from the HHS Office for Civil Rights lately regarding the upcoming resumption of OCR's audits. In early April, many received a request to confirm contact information, and last month another "blast" was sent out to the same CEs, this time requesting that they complete a fairly simple "pre-audit survey."

"Initially, they said they would send 800," says Chris Apgar, president of Apgar & Associates, but based on what he's been hearing, "it seems like they sent a lot more than that." In fact, the number may be as high as 10,000.

Among Apgar's clients alone, 10% or so received the emails, and in the case of a health plan, about eight separate components of the plan, including behavioral health clinics, received them.

In April, OCR resumed its long-delayed, congressionally mandated program to audit for compliance with the privacy, security and breach notification regulations *(RPP 4/16, p. 1)*. This follows OCR's completion in 2012 of what it called a "pilot" audit of 115 entities — all CEs *(RPP 7/12, p. 1)*. That project found widespread noncompliance and

formed the foundation for the permanent program *(RPP 3/13, p. 1)*.

With Phase II, OCR expands the audits to encompass business associates (BAs) for the first time, and is mixing things up a bit more, by establishing three separate "rounds" of audits. The audits will be based on a revised version of a "protocol" OCR used in 2012, which has 79 measures for privacy, 72 for security and 19 for breach. The revision was released on April 10.

Round I, underway now, involves CEs, while Round II, expected in 2017, will target BAs. Both of these rounds are expected to be desk audits, meaning no one will come on-site and auditees will be required to upload documents for review by OCR contractors.

Round III, although farther off, is what is making CEs so panicky, says Apgar. While desks audits might not turn out to be a big deal, those conducted in Round III (on-site audits) are putting CEs and BAs at high risk of enforcement action by OCR, says Apgar, especially if instances of "willful neglect" are uncovered.

The OCR emails are designed to create a pool of potential auditees, with perhaps 200 to 250 ultimately selected. OCR has not said how many will be desk vs. on-site audits.

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, Theresa Defino; Executive Editor, Jill Brown; Associate Editor, Lauren Clason; Publisher, Richard Biehl; Marketing Director, Donna Lawton; Fulfillment Manager, Tracey Filar Atwood; Production Director, Andrea Gudeon

Subscriptions to *RPP* include free electronic delivery in addition to the print copy, e-Alerts when timely news breaks, and extensive subscriber-only services at www.AISHealth.com that include a searchable database of *RPP* content and archives of past issues.

To order an annual subscription to **Report on Patient Privacy** (**$554** bill me; $524 prepaid), call 800-521-4323 (major credit cards accepted) or order online at www.AISHealth.com.

Subscribers to *RPP* can receive 12 Continuing Education Credits per year, toward certification by the Compliance Certification Board. Contact CCB at 888-580-8373.

The CEs selected for the first round should be notified within two months, Apgar says. So those CEs that received the confirmation email and survey should get ready in case they are selected. All others might want to review the protocol anyway.

"The time is now to address compliance gaps," he says, noting that such action could help prevent a breach or OCR investigation in the future.

OCR officials have publicly called attention to the fact that the request for documents received during a desk audit must be fulfilled within 10 days of receipt. And given that the audit protocol is already out, they have been advising CEs and BAs to measure themselves against the protocol.

At the recent HIPAA Summit in Washington, D.C., Rebecca Williams, chair of the health information practice at Davis Wright Tremaine LLP, advised CEs and BAs to develop a game plan centered on an "audit response team" to quickly respond if a covered entity is audited *(RPP 4/16, p. 8)*.

Gather Evidence Now

"I am saying 'Don't freak out but make sure you have all the documents you need,'" says Apgar, who has been giving webinars about the audits to groups such as the Oregon Medical Association.

During an audit, CEs will be required to demonstrate "continued compliance," which means offering evidence that goes beyond proving policies and procedures. Among the documents CEs and BAs might need to have on hand are screen shots, audit logs, monitoring reports, risk analyses, disaster recovery and emergency operations, and documentation that employees have been sanctioned for HIPAA infractions.

But Apgar has his own concerns, saying he has "more questions than answers."

Many of the performance measures in the protocol, which reads like instructions to an auditor, will require subjectivity on the part of the auditor, who may or may not have health care expertise. Some requests are vague.

For example, the protocol requires the auditor to "obtain and review access requests which were granted (and documentation of fulfillment, if any) and access requests which were denied." But it doesn't specify how many requests will be reviewed or over what time period, and if the auditor can simply request a sample. Such vagaries, he says, make preparation difficult.

Apgar reserves more of his anxiety for how OCR will handle the on-site audits. In the desk audits, CEs and BAs are expected to be audited for the notice of privacy practices and right of access under the privacy category; for their risk analysis and risk management under the security category; and content and timeliness of notifica-

tion under breach. But with on-site audits, OCR intends to conduct a "comprehensive" audit using the entire protocol and has not yet said how this would work, says Apgar.

Contact Apgar at capgar@apgarandassoc.com. ✧

For the Third Time, OCR Weighs In on Allowable Fees for Patient Records

Quick question for health care organizations: *What's the easiest way to get a patient mad at you?*

Follow-up question: *What's the easiest way to get the HHS Office for Civil Rights (OCR) mad at you?*

The answer to both questions appears to be: getting between patients and their records. On May 23, OCR issued its third missive about patient access, addressing the question of flat fees for copies of records. This follows separate FAQs issued in January and February.

For years, patients have complained to OCR about this. In fact, the lack of patient access to protected health information (PHI) is the third most common compliance issue that has triggered OCR investigations and enforcement actions since 2003, when the privacy rule went into effect. The top reason is impermissible uses and disclosures, followed by a lack of safeguards.

In 2014, *RPP* documented widespread violations of the access requirements that went into effect in 2013, such as providing patients with access to electronic copies of their PHI, and in the "form and format" they desire. Fees charged were also not in line with the regulations *(RPP 6/14, p. 1)*.

OCR officials knew there was a problem and frequently admonished covered entities (CEs) in somewhat informal ways in years past. But now it is getting serious, and CEs and business associates would be wise to finally pay attention because evidence indicates many of their current policies and procedures on records access violate the regulations.

Agency officials have acknowledged, and are now trying to address, the lack of specificity in the regulations around these issues, which has fed some of the noncompliance. But now that the guidance is out, OCR intends to bring more enforcement actions on this issue, *RPP* was told.

Taken together, the new documents underscore OCR's impatience with CEs that continue to stand in the way of patients accessing their records, a situation OCR Director Jocelyn Samuels says "must change." She adds: "[F]ar too often, individuals face obstacles to accessing their health information."

The access regulations changed in 2013, but not all CEs changed their policies as needed. Under the "new" regulations, for example, the time to respond to a request (not fulfill it) is 30 days instead of 60, and CEs must now make the information held electronically available to patients in the "form and format" that they want *(RPP 4/13, p. 1)*.

The guidance documents issued in January addressed "the scope of information covered by HIPAA's access right, the very limited exceptions to this right, the form and format in which information is provided to individuals, the requirement to provide access to individuals in a timely manner, and the intersection of HIPAA's right of access with the requirements for patient access under the HITECH Act's Electronic Health Record (EHR) Incentive Program" *(RPP 2/16, p. 1)*.

What might have taken CEs by surprise was the clear mandate to communicate by email with patients, even if the CE deems the mode to be "not secure." They are not required to use encrypted messages, for example.

Issued in February, the second set of FAQs stresses that "individuals can be charged only a reasonable, cost-based fee for the labor and supplies associated with making the copy, whether on paper or in electronic form." OCR also said "the right to have information sent directly to a third party empowers individuals to send their information wherever they want it to go."

HIPAA Trumps State Laws

Importantly, CEs may not charge fees that are allowed under their state laws unless they are also allowed under HIPAA, according to the February guidance. OCR reiterates that "labor (e.g., for search and retrieval) or other costs not permitted by the Privacy Rule may not be charged to individuals even if authorized by State law."

Further, patients who want their records transferred for purposes of treatment, payment and health care operations do not have to submit a formal request or pay a fee, OCR says.

The privacy rule "permits covered entities to disclose PHI for treatment, payment and health care operations without the need to first obtain an individual's authorization or receive an access request by the individual to have the individual's PHI directed to a third party for such purposes. See 45 CFR 164.506," the guidance states. "As a result, if an individual is seeking to have her PHI shared among her treating providers, the covered entities can and should do so; the individual should not have to facilitate this transmission by submitting an access request (and potentially having to wait up to 30 days for the information to be sent and be charged a fee) or by executing a HIPAA authorization."

The newest FAQ was issued three months after the February batch.

continued

"Today, in response to questions received after release of the guidance, OCR provides further clarification about the amount that an individual may be charged for a copy [of their PHI]," OCR announced on May 23. "Specifically, we clarify in a new FAQ that $6.50 is not the maximum amount that can be charged for all individual requests for a copy of PHI under the right of access."

OCR explains that CEs may impose a flat fee "not to exceed $6.50" if they choose not to "go through the process of calculating actual or average costs for requests for electronic copies of PHI maintained electronically as permitted by the Privacy Rule."

As OCR notes in its January FAQ, CEs may charge only for the following items: "(1) labor for copying the PHI requested by the individual, whether in paper or electronic form; (2) supplies for creating the paper copy or electronic media (e.g., CD or USB drive) if the individual requests that the electronic copy be provided on portable media; (3) postage, when the individual requests that the copy, or the summary or explanation, be mailed; and (4) preparation of an explanation or summary of the PHI, if agreed to by the individual."

CEs cannot, OCR says, impose fees for "costs associated with verification; documentation; searching for and retrieving the PHI; maintaining systems; recouping capital for data access, storage, or infrastructure; or other costs not listed above even if such costs are authorized by State law," nor for "clerical," "administrative" or "per-page" fees if the information isn't kept on paper.

Ultimately, the pricing method is up to covered entities, as long as it is "within the boundaries of what is permissible under the Privacy Rule," OCR says in the new FAQ.

For all of the FAQs on access, see http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html.

Tools for Consumers Are on the Way

As helpful (or more confusing, as the case may be) as CEs may find the access documents, they may do little to help patients who are confused about their rights, and whose dissatisfaction could prompt a complaint to OCR.

The agency promised in February that it would put out materials for patients, saying officials "continue to work with our colleagues to produce consumer-friendly resources, including sample communications tools, to encourage patients to access their health information."

OCR says it hopes that "these new materials will engage and empower patients to take control of their health care decisions, improving the quality of care they receive and leading to a better overall health care delivery system."

Prior to Samuels' arrival at OCR, then-director Leon Rodriguez tried to educate patients on access rights several times. In May 2012, he issued a "memorandum" to patients about this; it has since been reissued under Samuels' name (see http://www.hhs.gov/sites/default/files/righttoaccessmemo.pdf).

A year later, OCR launched a public awareness campaign, "Information is Powerful Medicine," which encouraged patients to request their medical records to better manage chronic conditions, such as HIV *(RPP 6/13, p. 1)*. ✧

Joint Commission Permits Text Orders, but Requires Safeguards

HIPAA compliance officers who have been fighting undercover or unapproved text messaging of orders by physicians may find an unexpected ally in the Joint Commission, which recently reversed its 2011 text messaging ban on orders, but only if an order is sent via a "secure text messaging platform."

"Hospitals shouldn't put their head in the sand and ignore the fact that text messaging is used by health care providers," says Richelle Marting, an attorney with the Forbes Law Group in Overland Park, Kansas. "The Joint Commission's revised position on texting orders enables hospitals to face the issue head-on and ensure it's done correctly."

In the May issue of *Joint Commission Perspectives*, Joint Commission officials said that "effective immediately, The Joint Commission has revised its position on the transmission of orders for care, treatment, and services via text messaging for all accreditation programs. Licensed independent practitioners or other practitioners in accordance with professional standards of practice, law and regulation, and policies and procedures may text orders as long as a secure text messaging platform is used and the required components of an order are included."

The Joint Commission said hospitals may allow texting on a platform that includes a "secure sign-on process, encrypted messaging, delivery and read receipts; date and time stamp; customized message retention time frames; [and] specified contact list for individuals authorized to receive and record orders."

The earlier kibosh on text messaging came as part of an FAQ issued five years ago. At that time, the Joint Commission explained in the new announcement, "[s]ending orders via text messaging was prohibited due to concerns about using personal mobile devices to send unsecure text messages between providers. In addition, texting applications were unable to verify the identity of the person sending the text or to retain the original message as validation of the information entered into the medical record." Advances in technology have alleviated these concerns, the Joint Commission said.

But it isn't giving organizations free rein with using text messaging for orders.

The Joint Commission also wants accredited organizations that permit texting of orders to comply with the Medication Management Standard MM.04.01.01, which addresses the elements of a complete medication order and how to handle incomplete or unclear orders.

In allowing the texting of orders, organizations need to establish policies that "specify how orders transmitted via text messaging will be dated, timed, confirmed, and authenticated by the ordering practitioner. Additionally, organizations need to consider how text orders will be documented in the patient's medical record," the Joint Commission said.

It also suggested that organizations may adapt its requirements for verbal orders that address the Provision of Care, Treatment, and Services Standard PC.02.01.03 and Record of Care, Treatment, and Services Standard RC.02.03.07.

Covered Entities Need Broader Policies

Texting can be addressed in institutional policies, such as medical staff bylaws, Marting says. Adherence to the Joint Commission standard could be a condition of medical staff privileges, with noncompliance leading to disciplinary action.

The Joint Commission's new position refers only to ordering by text messages and does not address other types of texting. HIPAA covered entities need to comply with the privacy, security and breach regulations as they relate to all kinds of texting that, like orders, may involve the use and disclosure of protected health information (PHI).

HIPAA consultant Frank Ruelas, for example, has decried a lack of texting policies despite the rampant use of this practice by CEs. Ruelas, principal of HIPAA College and a facility compliance professional at St. Joseph's Hospital and Medical Center, which is part of Dignity Health in Phoenix, Ariz., says the belief that "texting allows for a higher quality of care, better patient safety, increased levels of communication" is not backed up by data *(RPP 1/16, p. 1)*.

For more information, see www.jointcommission.org/assets/1/6/Update_Texting_Orders.pdf. Contact Marting at rmarting@forbeslawgroup.com and Ruelas at Frank@hipaacollege.com. ✧

Solid Contingency Plans Are Key to Weathering Damaging Conditions

Effective contingency plans are crucial for covered entities (CEs) to ensure patients have uninterrupted access to care and protected health information (PHI) in the event of unforeseen events or conditions.

The HIPAA security rule mandates the development of a contingency plan under administrative safeguards (45 CFR §164.308(a)(7)), which would be used in case of events including "fire, vandalism, system failure, and natural disaster." The rule lists several components of a proper contingency plan:

"(A) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

"(B) Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data.

"(C) Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

"(D) Testing and revision procedures (Addressable). Implement procedures for periodic testing and revision of contingency plans.

"(E) Applications and data criticality analysis (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components."

Jay Hodes, president of Virginia-based Colington Security Consulting LLC, says most of his clients do not have a proper contingency plan in place. Many don't even realize it's a HIPAA requirement, much like a risk assessment.

"There is a lot that goes into it that providers would need to look at," Hodes says. "But then again, I think there is some continuity of business operations that providers need to consider."

Timelining everything (i.e., mapping out which systems come back online first, including business operations not pertaining to PHI), helps staffs prioritize and work effectively, Hodes says. Keeping up with regular precautionary measures is also critical — one client that suffered a black-out from a tornado credited

its contingency plan for being able to get back up and running, partly because the plan called for regular back-ups to the cloud.

Hodes tells his clients to "what-if" possible scenarios to death when developing a contingency plan, then tailor it to accommodate any and all plausible situations they can come up with. Chances are CEs still won't think of everything, according to J. Ira Bedenbaugh, a principal at Elliott Davis Decosimo LLC, based in South Carolina, but they have to try.

When floods ravaged South Carolina in October 2015, Bedenbaugh says, several hospitals across the state lost water. Those hospitals had planned to lose electricity, but the loss of water took them by surprise. "A lot of time in contingency plans, we limit our thinking of what the contingencies could be," he says.

Another issue is that, while an organization might have a contingency plan, often the person who designed it is the only one who knows it exists. "Often they're in the head of somebody within the practice," Bedenbaugh tells *RPP*. "They're just not documented."

That's a problem when that person can't make it into the office because of icy roads or other poor weather conditions, leaving the rest of the staff in the dark, sometimes literally. "It could be as simple as...they just don't know who to call," Bedenbaugh says, who recalled one client whose privacy officer was out for weeks after a car accident. "Or it could be as complex as they don't have

The Strike Team Approach to Contingency Planning

In their chapter for *RPP* readers on "Contingency Planning, Business Continuity and Disaster Recovery," Joseph Arnett and Russ Arnett of Taxation Professionals, Inc. describe in detail this "strike team" approach to contingency planning. To access the full 43-page chapter — and more than 20 detailed treatments on HIPAA privacy and security issues available only to *RPP* subscribers — go to the subscriber-only Web page at https://aishealth.com/newsletters/reportonpatientprivacy and click on "Privacy and Security Compliance Guides" under "Subscriber Services" in the right column. For more information, contact Russ Arnett at Russ.Arnett@Taxation-Pros.com or (562) 881-4921.

Every department within any organization has its "expert," and if it is lucky it has experts that are multi-talented, and if it is really lucky, it has multi-talented experts that are willing to be part of or lead a "Strike Team." The authors highly recommend the Strike Team approach.

To get these prime players and back-ups to be leaders or members of a strike team takes a combination of knowing the company and department dynamics and being a good sales person.

Usually these experts are "company people," so being able to help would be a natural thing for them, and the issue is simply that no one has asked.

In a perfect set of circumstances these teams could be identified after management has bought into the concept of "Let's keep the company going after a crisis," but unfortunately it takes actions from the people who really are the "heart and soul" of the company to get the point across.

The "ground-swell" concept could work to the entity's advantage if senior management is not buying into the importance of contingency planning. Start with what you consider the primary "critical" department, and work with them to get a small and powerful team with back-ups.

This will provide you with a base to provide some upward motivation by developing newsletters and training times. Remember that small, smart, motivated teams are the best.

The Three Levels of Strike Teams

There are three levels of "Strike Teams," and for a business to recover quickly, it is the authors' view that they all are critical. The teams have some of the same characteristics:

- The members have expert knowledge in more than one area.
- The members are willing to be involved in the recovery.
- The members can step up to a leadership role if necessary.
- The members must all be trained and certified in basic Red Cross medical skills.

Each of the levels also has specific authority and responsibilities.

usernames or passwords that they might need to reboot systems, or things like that."

Contingency plans should be published someplace where the staff knows where to find them, and they should be practiced, practiced, practiced, although that might hold different meaning for different organizations.

"If you look at larger health care organizations, they probably test and drill all the time. But for smaller organizations, the reg is all for testing but you're going to have to work hand-in-hand with your IT company if you were to take down your system and try to reboot, or try to do some type of virtual VPN access — making sure everything works, making sure if you are utilizing VPN, that there is accessibility, that the firewall isn't going to kick you out or that there's some other type of software on the system," Hodes says.

He adds that smaller CEs are probably better off contracting with outside IT vendors. "They have to take the IT component seriously."

Tests should be ongoing, too, as the environment changes, Bedenbaugh says. "You just can't do it once."

OCR could penalize CEs for not having a contingency plan in place, especially if a patient needs access to his or her PHI for something serious, such as a surgical procedure.

"While the contingency plan is probably not the end reason why they're penalized," Bedenbaugh says, "you could see under certain circumstances that not having a proper contingency plan in place could lead to penalties because of failure to meet some other requirements."

Contact Bedenbaugh at ibedenbaugh@elliottdavis.com and Hodes at info@colingtonsecurity.com. ✧

The Strike Team Approach to Contingency Planning (continued)

Level One – Executive Level Team Members

The Level One Strike Team members —

- can make the financial decisions and have appropriate board of director's approval to operate the business in a crisis mode;
- are responsible for all media communications and have the skills for interfacing with all levels of media;
- are responsible for determining areas to relocate and have the authority to enter into leases or rental agreement; and
- are responsible for maintaining and invoking internal communication emergency protocol.

Level Two – Senior Management Level Team Members

The Level Two Strike Team members —

- can manage recovery teams;
- can obtain immediate need supplies and equipment;
- understand the corporate needs and priorities;
- can stand in for level one management; and
- must have the ability to cover more than one critical area if needed.

Level Three – Operational Teams

The Level Three Strike Team members —

- include management and direct knowledge experts;
- must have outside contacts that will support recovery efforts;
- must have skills to maintain relationships with outside emergency crews;
- must be able to communicate remotely if needed; and
- must have strong and direct communication skills to assure that issues discovered are documented and addressed in the appropriate priority sequence.

These teams would be identified on the recovery plans as the primary contacts and call out members for the department that they cover and serve.

Ponemon: Data Breaches Could Cost Industry as Much as $6.2 Billion

Health care organizations are improving — albeit slowly — in terms of breach prevention resources and technological expertise, yet the number of breaches has remained roughly the same, according to the latest study conducted by the Ponemon Institute LLC and sponsored by ID Experts Corp.

Ponemon estimated that data breaches are costing the health care industry as much as $6.2 billion a year, and reported that 89% of covered entities (CEs) that participated in its *Sixth Annual Benchmark Study on Privacy and Security of Healthcare Data* had experienced at least one breach in the past five years. Forty-five percent of CEs had more than five breaches in the past two years. By contrast, 61% of business associates (BAs) had at least one, and 28% had more than two.

Ninety-one CEs and 84 BAs responded to the survey. On average, a data breach cost CEs $2.2 million over the past two years and resulted in the exposure of 3,128 records. BAs, on the other hand, paid out around $1 million on average for breaches that exposed an average of 5,887 records.

For the second year in a row, criminal attacks were the leading cause of breaches. Half of CEs and 41% of BAs blamed hackers for data breaches. "Malicious insiders" accounted for 13% of CE breaches and 9% of BA breaches.

Increased Resources Don't Yield Results

Last year's study distinguished between electronic and paper "security incidents," so it's hard to compare this year's overall data breach figures to last year's, but ID Experts President Rick Kam said in a May 17 webinar that he's concerned about how the number of breaches is not decreasing to correspond with a reported increase in investments in both resources and expertise. "With all the improvement we discussed, it seems that number should go down, but it really doesn't," he said.

Larry Ponemon, Ph.D., founder and chairman of the Ponemon Institute, echoed those sentiments. "If you ask the question 'what is most important?,' it's that there's really no change," Ponemon said during the webinar. "What's surprising is, with all the media coverage of the health care industry and these major mega-data breaches like Anthem and others, you think that would drive organizations to a higher level of security performance or security posture."

Industry Is Taking 'Baby Steps'

Ponemon acknowledged that the industry is taking "baby steps" in the right direction. Sixty-three percent of CEs have data breach policies in place, the study found, an improvement over the 58% who reported having a plan in 2015. Fifty-seven percent report having adequate security expertise on their teams, up from 53% in 2015. While 30% of CEs and 32% of BAs said their security budgets have increased over the past two years, 52% of CEs and 50% of BAs reported it had actually decreased.

Perhaps one explanation for the disconnect is the immediate effect a major data breach has on the industry when it lands in the headlines — prompting organizations to shore up their defenses, which might be done either haphazardly or without a permanent commitment. For example, 60% of CEs and 54% of BAs say they assess vulnerabilities, but it's often done annually or without a set schedule.

Breaches Trigger 'Newfound Religion'

"What we find in lots of Ponemon Institute research is that organizations, in the aftermath of a cyber incident or a big data breach, get newfound religion and for a period of time, maybe six months to a year, an organization starts spending more to build up their security posture," Ponemon said.

There is a general shortage of qualified security personnel, too, Ponemon acknowledged, creating a "seller's market" within the industry. Only 57% of CEs said they had adequate IT expertise on their teams when it came to preventing and detecting data breaches, although that is an increase over the 53% who reported so in 2015. But confidence in their organization's ability to prevent and detect breaches is still woefully low — slightly more than half of CEs expressed confidence in their organization, while only 46% of BAs did.

"Generally speaking, people are just not that confident about their ability to detect all patient data loss or theft," Ponemon said. "It really becomes hard when you're talking about small numbers, one record here, 10 records there, but you have to have a system that captures that information."

Visit http://tinyurl.com/hp4fumz to access the report. ✧

CEs Face New Gender Bias Rule

continued from p. 1

"A lot of people's experience might be from the media," where people such as Jenner "are very much out there, talking and sharing information," Levasseur says. "But the story that maybe is not being told is there are thousands of transgender people who are living their lives privately and people do not know they are transgender. We don't want people to be afraid to go to the doctor…to be 'outed' in the waiting room."

The new rule follows an August 2013 request for information and a September 2015 proposed rule about which HHS received approximately 25,000 comments. It puts into practice "the first federal civil rights law to broadly prohibit discrimination on the basis of sex in federally funded health programs," HHS said when the rule was published May 18.

Application Is Quite Broad

HHS also issued a set of FAQs, which noted that the final rule "applies to every health program or activity that receives HHS funding, every health program or activity administered by HHS, such as the Medicare Part D program, and the Health Insurance Marketplaces and all plans offered by issuers that participate in those Marketplaces. Covered entities may include hospitals, health clinics, health insurance issuers, state Medicaid agencies, community health centers, physician's practices and home health care agencies."

OCR investigates complaints of the HIPAA privacy, security and breach notification rules as well as discrimination as outlined in Section 1557. Prior to publication of the final rule, OCR investigated discrimination in health care complaints based on the ACA itself, which has been in effect since 2010.

In July 2015, OCR announced a landmark settlement with The Brooklyn Hospital Center to resolve allegations that the facility had violated Section 1557 "when it assigned a transgender female who presented as a female at the hospital…to a double occupancy patient room with a male occupant."

The Brooklyn hospital agreed to adopt, and train employees on, new policies and procedures ranging from admitting and rooming to documenting patients' "legal and a preferred name" and their "gender and/or transgender status, if the Patient has identified that status and agrees that it should be recorded." Workers also had to become conversant with the meaning of terms such as "gender non-conformity" and "sex assigned at birth."

That settlement marked the first time OCR formally resolved an anti-discrimination complaint related to gender with a settlement *(RPP 8/15, p. 1)*.

The effective date of most provisions in the new rule is July 18, 2016, 60 days from its publication. According to the rule, changes in "health insurance or group health plan benefit design (including covered benefits, benefits limitations or restrictions, and cost-sharing mechanisms, such as coinsurance, copayments, and deductibles), such provisions, as they apply to health insurance or group health plan benefit design" must be ready to go into effect with the next plan year.

Among the few specific requirements are that CEs must develop and post a "nondiscrimination notice," much like a notice of privacy practices, to "inform individuals of their civil rights under Section 1577, and provide information on how to file a complaint. OCR provides a sample in the final rule, and states that this can be combined with other notices.

The notice must be posted within 90 days of the effective date of the regulation (by mid-November). Organizations are also required to designate a "compliance coordinator" and adopt grievance procedures for patients who believe they have been discriminated against. These two requirements are voluntary for organizations with 15 or fewer full-time workers.

OCR promised to "provide covered entities with training materials that will cover the key provisions of the regulation that can be used by entities in conjunction with their own training materials." These materials will be issued "prior to the effective date," OCR said, adding it expected to spend $10,000 on these materials.

New Rule May Be Difficult to Implement

But even when those documents arrive, the broad requirements will still prove difficult to implement in practice. To help, Lambda Legal and a host of other organizations and attorneys released an update to their November 2013 guidance, "Creating Equal Access to Quality Health Care for Transgender Patients: Transgender-Affirming Hospital Policies," to coincide with the release of the final rule. To download the guide, visit http://www.lambdalegal.org/blog/20160525_lgbt-advocates-revise-guidelines-hospitals-trans-patients.

The initial version of the guide formed the basis for many requirements OCR inserted in its corrective action plan with the Brooklyn hospital, and Lambda officials told *RPP* that OCR officials utilized the guide when creating the plan.

Levasseur says Lambda is working with OCR now to distribute the new version. The agency did not respond to *RPP*'s requests for comment on the guide.

Among the additions in the revised Lambda guide is a section on "Collection of gender identity data in electronic health records." This is key because the rule, as

noted, requires access to, and the provision of, care that matches the patient's gender identity.

According to the rule, "*Gender identity* means an individual's internal sense of gender, which may be male, female, neither, or a combination of male and female, and which may be different from an individual's sex assigned at birth. The way an individual expresses gender identity is frequently called 'gender expression,' and may or may not conform to social stereotypes associated with a particular gender. A transgender individual is an individual whose gender identity is different from the sex assigned to that person at birth."

OCR addressed this issue in the preamble of the new rule. "We understand that, in some instances, a covered entity may need to ask transgender enrollees for additional information, including information related to their biological sex or sex assigned at birth, to facilitate overriding denials of coverage for sex-specific health services due to gender billing code mismatches in their computer systems," OCR said.

"We clarify in this preamble that a covered entity is permitted to ask transgender enrollees to provide such additional information, as long as the covered entity does not unduly burden enrollees or make unreasonable inquiries that serve to delay their receipt of coverage. In addition, we clarify that it is permissible for a covered entity to request information about the biological sex of the applicant on an insurance application form to assist the covered entity in identifying the medical appropriateness of sex-specific health services," it said.

Collecting Gender Identity Is a Must

But OCR added that the information requested cannot be "used in a discriminatory manner," and the CE must comply with "applicable HIPAA privacy requirements." This means that knowledge of a patient's gender or transgender status should be shared only with those who need to know and must be restricted based on the patient's preference, and information obtained should meet the minimum necessary standard.

The Lambda guide recommends the following be incorporated into privacy policies and procedures:

◆ "Every physician, [Hospital] employee and contractor who uses, discloses, or requests patient information, including information regarding a patient's gender identity or expression, transgender status, or other demographic data, on behalf of [Hospital], shall make reasonable efforts to limit disclosure of and requests for protected health information to any person not directly involved in the treatment of a particular patient to the minimum necessary to accomplish the authorized purpose of the use, disclosure, or request, in accordance with applicable federal law and regulations, including minimizing incidental disclosures. Procedures appropriate for implementing this policy vary based on the intended purpose of the use, disclosure, or request, as provided elsewhere in this HIPAA Privacy Procedure Manual."

◆ "[Hospital] will ensure that every physician, [Hospital] employee and contractor will have access to protected health information only to the minimum extent necessary and relevant to perform his or her specific job functions, as described in this HIPAA Privacy Procedure Manual."

The Lambda guide also recommends that intake forms, either electronic or paper, have several options for patients regarding gender identity and have two steps:

(1) First the patient is asked, "What is your current gender identity?" Answers could be —

- Male
- Female
- Female-to-male (FTM)/Transgender Male/Trans Man
- Male-to-Female (MTF)/Transgender Female/ Trans Woman
- Genderqueer, neither exclusively male nor female
- Additional Gender Category/(or Other _____)
- Decline to answer

(2) The second question is "What sex were you assigned at birth on your original birth certificate?" Patients are to select one: male, female or decline to answer.

Discrimination Triggered a Privacy Violation

CEs could also glean some insights based on a review of previous actions on gender discrimination that OCR has taken, the most detailed of which is the settlement with the Brooklyn hospital. But OCR has also collected other "sex discrimination case examples" on the agency's website (see http://www.hhs.gov/civil-rights/for-individuals/section-1557/ocr-enforcement-section-1557-aca-sex-discrimination/index.html).

Among the other cases is one that shows how possible HIPAA and nondiscrimination violations may overlap or actually cause one or the other to occur.

According to OCR, Avera Marshall Regional Medical Center in Minnesota treated "married individuals differently on the basis of sex. If the patient was male, he was automatically listed as the guarantor for billing purposes. However, if the patient was female, the Center automatically assigned the patient's husband as guarantor," OCR said, without providing details as to when this situation occurred.

As a result of OCR's investigations, the medical center "subsequently changed its billing process to list the patient as the guarantor of his or her bill and allow parents to choose the guarantor of their minor children" and "implemented a new restrictions policy and provided training to staff on the policy" so that such disclosures would not occur in the future.

A portion of the rule addresses "meaningful access for individuals with limited English proficiency." Privacy issues are prominent here as well, as the rule mandates that language assistance services "must be provided free of charge, be accurate and timely, and protect the privacy and independence of the individual with limited English proficiency."

Further, the rule prohibits the use of a patient's family or friend for translations or language assistance. "For communications of particularly sensitive information, oral interpretation by an individual's family or friend often also implicates issues of appropriateness, confidentiality, privacy, and conflict of interest. Thus, covered entities may not rely on family members, friends, or other informal interpreters to provide language access services unless the situation meets an applicable exception in § 92.201(e)(2)-(3) of the final rule," which refers to instances where danger is imminent or when the patient requests this.

Chris Apgar, president of Apgar & Associates, a HIPAA consulting firm, told *RPP* the rule "is not going to be easy to implement," and he laments that it has not yet been on CEs' radar screens. Apgar also faults the regulation for lack of specificity, saying he hopes OCR will issue guidance in the future.

The Lambda guide "takes the health care provider community a long way down the road" toward understanding the nuances of complying with the regulation and preventing lawsuits and complaints based on gender discrimination, says Apgar.

View the law and related materials at: http://www.hhs.gov/civil-rights/for-individuals/section-1557/nondiscrimination-health-programs-and-activities-proposed-rule/index.html.

Contact Dru Levasseur through Eseosa Olumhenseough at eolumhense@lambdalegal.org and Apgar at capgar@apgarandassoc.com ✧

PATIENT PRIVACY COURT CASE

This monthly column is written by Jenny Harrison of Morgan, Lewis & Bockius LLP in San Francisco. 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 Jenny at jenny.harrison@morganlewis.com.*

◆ **Court finds a whistleblower's disclosure of privately insured patients' PHI in a False Claims Act action did not violate employer's confidentiality agreement.** On May 13, 2016, the U.S. District Court for the Northern District of Illinois dismissed the defendant's single counterclaim in *U.S. ex rel. Cieszyski v. LifeWatch*, No. 1:13-cv-04052 (N.D. Ill. 2016), stating that protecting the whistleblower outweighed the employer's expectations in protecting its confidential information. In the initial action, a certified technician ("Cieszysnki") working at LifeWatch Services, Inc. sued LifeWatch for False Claims Act violations based on LifeWatch's submission of false claims to the government for reimbursement for heart monitoring services. LifeWatch filed a counterclaim alleging that Cieszysnki breached the confidentiality agreement he signed when first employed at LifeWatch and the company privacy policy he received several years later, both of which forbade the disclosure of confidential information or protected health information (PHI). The counterclaim was based on Cieszysnki's disclosure of LifeWatch's confidential information to the government in the False Claims action, including a spreadsheet containing PHI for approximately 52,000 patients, some of whom were not insured by government insurers and therefore were not related to Cieszysnki's False Claims action. Strong public policy favors protecting whistleblowers from retaliation to prevent any chilling effect on attempts to uncover fraud against the government. A court must balance this public policy against an employer's legitimate expectations in protecting its confidential information. After conducting this balancing test here, the court held that LifeWatch failed to state a claim for breach of the confidentiality agreement since it was "unrealistic" to impose a burden on a plaintiff to know precisely how much information should be provided to the government when reporting a claim of fraud and because Cieszysnki did not disclose any information beyond that which was necessary for his action. The court also held that LifeWatch failed to state a claim based on breach of the privacy policy because LifeWatch failed to show how a policy received several years after commencing employment was part of the employment agreement.

PRIVACY BRIEFS

◆ **U.S. District Judge Richard Bennett on May 27 dismissed a lawsuit against CareFirst, Inc. over a data breach that affected more than 1 million customers.** The judge concluded the two plaintiffs had not proven any actual injury had resulted from the breach of their protected health information (PHI). The decision came just as U.S. District Judge Lucy Koh allowed the Anthem, Inc. breach lawsuit to move forward. Read the CareFirst opinion with your PACER login at http://tinyurl.com/jgjy5gn.

◆ **Negative Yelp reviews are prompting some doctors to breach HIPAA in defending themselves in their responses,** ProPublica reported on May 27. The news outlet recently partnered with the ratings site to gain access to its database of reviews, finding that doctors are using the public forum to clarify inaccuracies in patients' reviews and scolding them for blaming physicians for their own poor health decisions. ProPublica found that dozens of the responses prompted accusations of HIPAA violations. Visit http://tinyurl.com/jc3h7sd.

◆ **Hackers that besieged Kansas Heart Hospital refused to return full access after the hospital paid the ransom,** news station KWCH reported on May 20. The hospital's president declined to say how much it paid, but said it was "a small amount." When the hackers demanded a second payment, the hospital refused. Visit http://tinyurl.com/gl3uvhd.

◆ **Four patients filed a complaint with HHS against Salt Lake City-based genetic testing company Myriad Genetics, Inc., saying the company is refusing to give them their full test results,** *Stat News* reported on May 19. Gene-testing companies and doctors frequently ignore a large chunk of genotype data that has no known clinical significance. At least one of Myriad's patients wants to contribute her full genome to a genetic databank. Myriad bowed slightly after the patients filed the complaint, sharing some additional information, though not all it has. Myriad issued a statement saying it believed it had complied with the patients' request and the complaint therefore lacks merit. Visit http://tinyurl.com/hv3bsct.

◆ **California Correctional Health Care Services notified approximately 400,000 patients on May 13 that an unencrypted laptop had been stolen from an employee's car on April 25.** The laptop was password-protected and had files on patients incarcerated between 1996 and 2014. The company said it did not know if the computer contained any sensitive information. Visit http://tinyurl.com/jdhnqq7.

◆ **A cyberattack at Medical Colleagues of Texas, LLP may have compromised more than 68,600 patient records,** the clinic reported to the HHS Office for Civil Rights on May 11. The provider first noticed "unusual activity" on its network on March 8, which prompted the clinic to launch an internal investigation and seek outside help in determining if hackers had gained access to its systems. Exposed data included names, addresses, health insurance information and Social Security numbers. Visit http://tinyurl.com/jgmrabq.

◆ **Illinois Gov. Bruce Rauner (R) on May 6 signed into law HB 1260, which expands breach notification requirements to any entity, including websites and mobile applications, that collects and handles nonpublic personal information.** This includes everything from login credentials to biometric information. Only California, Florida and Nebraska have similar privacy laws, according to law firm Alston & Bird. Visit http://tinyurl.com/gvjgb6x.

◆ **Florida-based Eye Associates of Pinellas on May 5 notified OCR and more than 87,300 patients that one of its vendors had been hacked.** Software vendor Bizmatics, Inc. alerted the eye clinic to the breach on March 30, saying that "at least some" of its patient files had been affected. The vendor said the breach occurred in January 2015 and that it was unable to determine what files had been accessed. Compromised PHI potentially included names, dates of birth, addresses, phone numbers, insurance information and Social Security numbers. Visit http://tinyurl.com/hsctsop.

◆ **Because data breaches don't have a major impact on revenues, health care organizations aren't financially incentivized to invest the resources necessary to prevent them,** according to a May 5 report from the Brookings Institution. In interviews with 22 industry executives, the think tank concluded that too many people have access to the data that health care companies store, and that the data are stored for too long. Brookings recommended that OCR better communicate details of its audits to the public, and create a universal HIPAA certification program. Visit http://tinyurl.com/hkm8pu9.

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 provide regular access to the newsletter — and other subscriber-only resources at AISHealth.com — 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.)