Report on
PATIENT PRIVACY

Volume 17, Number 1 • January 2017

Practical News and Strategies for Complying With HIPAA

Contents

In Rare State HIPAA Action, New York Attorney General Gives 'Angels' a Win

A 16-year-old Rochester, N.Y., home health agency called "Angels in Your Home" apparently had something short of a heavenly soul under its roof, according to the New York State Attorney General (NYAG), who alleges a former CEO "unlawfully" phoned patients after helping to establish a rival firm called "All-American Health Care" (AAHC).

Obtaining and using the phone numbers to try and switch patients to the new firm was a HIPAA violation, according to the NYAG, and resulted in a $25,000 penalty and settlement between the NYAG and AAHC related to actions by its CEO Marco Altieri, the former CEO of Angels. The settlement also accuses AAHC of violating a state law.

In his Dec. 23, 2016, announcement of the settlement, NYAG Eric Schneiderman said AAHC also agreed to an "injunction permanently prohibiting them from violating HIPPA (sic) laws."

The case may represent a new enforcement target for the NYAG, and perhaps other states will take note. Yet the interesting situation is not clear-cut. Dan O'Brien, an attorney for AAHC, tells *RPP* the firm admitted to no wrong-doing and provided a copy of the settlement to support his contention.

"[A]s far as we are aware, this case is the first instance in which an approved fiscal intermediary has been alleged to have violated HIPAA for simply obtaining contact information," adds O`Brien, a partner with Woods Oviatt Gilman LLP. "My clients were assured that this interpretation of the HIPAA regs would be applied to other fiscal intermediaries throughout the State."

continued on p. 10

Under the New Administration, OCR May Face Restraints or Keep 'Flying Free'

Following his expected confirmation, HHS Secretary-designate Tom Price will name a new director of the Office for Civil Rights (OCR), as current leader Jocelyn Samuels, a political appointee, steps down on Jan. 20. Covered entities (CEs) and business associates (BAs) may breathe a sigh of relief at the departure of Samuels, who presided over an unprecedented 13 enforcement actions that netted OCR nearly $25 million in 2016, more than double the agency's take in any single prior year *(RPP 12/16, p. 1)*

But whether the new director, endorsed by an administration vowing to be less burdensome to businesses, will suddenly tamp down on enforcement efforts is anyone's guess. Cases take years to develop and safeguarding patient privacy is generally a sacrosanct principle with Democrats and Republicans alike. And what isn't changing, at least so far, is that patient advocate Deven McGraw is still OCR's deputy director for patient privacy *(RPP 7/15, p. 8)*.

"Will the new administration allow OCR a free hand to negotiate settlements with health care providers and others in the health care industry over alleged HIPAA violations involving high-dollar payouts? Or, will the agency see its wings clipped by re-

HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

Editor
Theresa Defino
Theresa.defino@hcca-info.org

quiring it to close investigations into large breaches that disclosed large amounts of patient health information behind the scenes through informal case resolutions?" muses HIPAA expert David Holtzman. "Only time will tell."

In any case, a new director won't be named right away, and in the interim an acting head will be in charge. To date that individual has not been identified. OCR is likely to issue few, if any, settlements before a new director takes the helm. The nation's top HIPAA official will need several months to become acclimated to the office. But this lull is no time to take a break on compliance, experts warn.

Price Supports Loosening Some Restrictions

The new appointee will be the seventh to head OCR since the agency was given the authority to enforce HIPAA 17 years ago, as previous directors have served an average of only two-to-three years.

In many ways, the incoming OCR director will have more duties and challenges than those that greeted even Jocelyn Samuels when she began in 2014, since the agency has additional duties under the new 21st Century Cures Act *(RPP 12/16, p. 7)*.

Report on Patient Privacy (ISSN: 1539-6487) is published 12 times a year by Health Care Compliance Association, 6500 Barrie Road, Suite 250, Minneapolis, MN 55435. 888.580.8373, www.hcca-info.org.

The new director will also be under pressure to keep up that pace, for fear that any slowdown might look like OCR is slacking off or isn't "serious" about enforcement anymore.

Whether President-elect Trump will have an impact on health IT and HIPAA is a big question, given his "positions on health information privacy and security are not well known," says Holtzman, who is vice president of compliance for the HIPAA consulting firm CynergisTek.

But Holtzman adds that incoming HHS Secretary Price, a physician, "has generally supported the development of health information technologies," while also a "frequent critic of what [Price] describes as burdensome regulations on health care providers."

Price, adds Holtzman, "sponsored legislation to scale back the reporting requirements" for the meaningful use electronic health records initiative.

"Dr. Price's legislative record also includes proposals to pare back current HIPAA privacy rule prohibitions on health insurers, giving employers who sponsor employee benefit programs information about employee and family health insurance claims and treatment records," says Holtzman. "If confirmed to lead HHS in a Trump administration, Dr. Price may take the department in a new direction concerning how it views HIPAA privacy protections."

Long Line of Short-Term Directors

As noted, Price may not move quickly to hire a new OCR director. "While the job is important, it is not politically sensitive," says Holtzman. "Senior staff who have been with the agency for many years" will step in.

Samuels became the director in August 2014 after serving as the acting assistant attorney general for the civil rights division in the Department of Justice *(RPP 8/14, p. 1)*. Samuels was appointed after her predecessor, Leon Rodriguez, became director of the U.S. Citizenship and Immigration Services in the Department of Homeland Security *(RPP 7/14, p. 1)*.

Rodriguez came on board in 2011, succeeding Georgina Verdugo, who served for just two years, beginning in September 2009 *(RPP 10/11, p. 1)*. At the time, Rodriguez was the deputy assistant attorney general and chief of staff in the civil rights division at DOJ. He was the first — and so far the only — OCR director who had some HIPAA experience, having gained familiarity serving as a county attorney and as an attorney in private practice where he had been a business associate.

Prior to Verdugo, OCR was headed by Richard Campanelli from 2002 to 2005, followed by Winston Wilkinson, who served from 2005 to 2009. Not since President Clinton was in office has an OCR director served more than four years. OCR was delegated authority for HIPAA

enforcement in 2000; the privacy rule went into effect in 2003 and the security rule two years later.

Adam Greene, a partner with Davis Wright Tremaine in Washington, D.C, and a former OCR regulator, says he expects the incoming OCR director to also "have more of a civil rights background" than HIPAA background, following in the line of previous directors. Even though she was new to HIPAA, Samuels won props from Greene for how engaged she was with the compliance community, noting in particular the number of public presentations she gave.

Some experts are confident that OCR will continue to produce, in the words of Reece Hirsch, "multi-million-dollar settlements." But Hirsch, a partner in the San Francisco office of Morgan, Lewis & Bockius LLP, also doesn't expect OCR to be the beneficiary of an increase in resources. It is important to note that OCR is able to pump the $24.7 million it collected last year into enforcement efforts.

The compliance community has a number of unmet needs that a new director must be attuned to. OCR "itself should invest more in providing clear guidance and in a timelier manner," says Chris Apgar, president of the HIPAA consulting firm Apgar & Associates.

For example, "the cloud security guidance released this year, touted as a high priority on OCR's agenda, took two years to make it out of OCR," Apgar said. "I understand things can move slowly when it comes to government but HIT is rapidly changing, risks are changing and so forth. Taking two years to publish 'top priority' guidance doesn't cut it."

Guidance, New Rules Could Stall

In the immediate future, OCR will not be free to issue new guidance "until the new secretary's leadership team, including an OCR director, is in place" to sign off on such documents, notes Holtzman.

OCR ended 2016 without issuing promised guidance, in fact. In October, McGraw said she hoped that, before the end of 2017, OCR would release "short guidance" to address the confusion that occurred after the mass murder in Orlando, Florida, last summer *(RPP 11/16, p. 3)*. At the time, the Orlando mayor said he had received a "waiver" from OCR to share information about patients with their friends and family members. McGraw also said guidance on texting and social media could be issued in the early part of this year.

And despite being ordered by Congress in the 2009 HITECH Act to do so, OCR has yet to issue guidance on the confusing concept of "minimum necessary."

Agencies issue more than just guidance; regulations are their primary output. Many have clamored for OCR to scrap the security rule entirely, arguing the incremental guidance documents, such as addressing cloud computing and the expected guidance on texting, are piecemeal additions to an outdated approach and framework.

But the presumed anti-regulatory bent of the new administration may put a chill on that, in addition to the appointment and expected confirmation of Rep. Mick Mulvaney (R-S.C), who is described as a "fiscal hawk," as the new head of the Office of Management and Budget (OMB).

OMB must approve all regulations and Mulvaney is expected to be particularly attuned to the cost of regulations. In addition, during the campaign, Trump pledged to repeal two regulations for every new one issued.

OCR is expected to continue moving forward with its audit program, and CEs and BAs should be taking steps to perform their own "self-audits," using all or parts of the protocol that OCR has put online *(RPP 4/16, p. 8)*.

Apgar hopes enforcement actions don't drop off under a new director. "OCR needs to continue with its enforcement efforts," he says. "The message needs to be made clear to the health care industry. HIPAA has been around well over a decade and CEs still don't seem to get the importance of information security. They believe they are doing well at privacy but you can't have good privacy without good security."

Discrimination, HIPAA Cases May Overlap

A new director will need to balance the agency's HIPAA duties with the more traditional — and larger — obligations of fighting discrimination in Americans' access to health care treatment and services. OCR also enforces the Civil Rights Act as it applies to federally supported health programs (which means everything from hospitals that accept Medicaid to health plans that accept Medicare), as well as new provisions under the Affordable Care Act (ACA).

Last summer, OCR issued a 200-page final rule implementing Section 1557 of the ACA, which prohibits discrimination on the basis of gender identity, alongside traditional prohibitions regarding race, color, religion, national origin, sex, disability and age *(RPP 6/16, p. 1)*. 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 "requires covered health programs and activities to treat individuals consistent with their gender identity."

In July 2015, OCR announced its first agreement related to a transgender patient, settling discrimination allegations leveled at Brooklyn Hospital Center (TBHC), which assigned "a transgender female who presented as

a female at the hospital…to a double occupancy patient room with a male occupant" *(RPP 8/15, p. 1)*.

Section 1557 has been in effect since the ACA was enacted but it was recently challenged in court. On January 3, 2016, OCR issued a statement via its list serv that it would continuing enforcing this section "to the full extent" allowable under a temporary injunction granted Dec. 31 in *Franciscan Alliance, Inc. et al. v. Burwell.* "The order preliminarily enjoins HHS from enforcing, on a nationwide basis, the provisions of the regulation implementing Section 1557 of the Affordable Care Act that prohibit discrimination based on gender identity or termination of pregnancy," OCR said.

"Section 1557 of the Affordable Care Act is critical to ensuring that individuals, including some of our most vulnerable populations, do not suffer discrimination in the health care and health coverage they receive. HHS is therefore disappointed by the Court's decision to preliminarily enjoin certain important protections against unlawful sex discrimination in our health care system," OCR said.

And a new window of OCR enforcement activity may be opening in 2017. Recent guidance issued by OCR spells out that health care organizations that use health information technologies, such as Internet patient portals, websites and health care apps, must make them accessible to people with disabilities.

The agency could be preparing to use its enforcement authority under the Americans with Disabilities Act to take action against health care facilities that have barriers to the accessibility of their health information technologies. Health information security officers will need to be assured that their fancy new apps comply with the privacy and security regulations, but also aren't discriminatory to the disabled.

Issued on Dec. 21, the new guidance can be found at http://tinyurl.com/z7op6ad.

Plea for Incentives

As far as selecting who might be the next OCR director, Price "needs to listen to the industry and consumers" when he makes a choice, says Apgar. A good director "needs to find a balance between enforcement and educating CEs, BAs and consumers," he says. The key is being able to "keep up with and appropriately respond to changes in the industry, changes in technology and changes in consumer demands such as more of what I would call mobile health or telehealth."

Rick Kam agrees the new director should work more with the health care industry, and offers some specific suggestions that he says could improve compliance.

"I would look to market incentives to drive more investment in health care security. The $32 billion invested to migrate from paper based records to electronic medical records did a lot to make this happen since the ACA," says Kam, who is president and co-founder of ID Experts, a security consulting firm and provider of credit monitoring services. "There was virtually no incentive to protect the records. I would consider OCR working with cyber insurance carriers to offer some form of incentives to increase investment in PHI data cyber security."

CEs Could be Incentivized to Protect PHI

He adds that the "idea of incentives could be financial, like lower premiums due to a lower risk rating from OCR or like what some cities do with restaurants with grades for cleanliness."

What OCR could do, Kam says, is "provide a grade for implementing HIPAA HITECH, security and privacy rule requirements. Or it could even be keeping score of how long since the last breach for an organization. All of these simple measures would drive behavior," says Kam.

Contact Holtzman at david.holtzman@cynergistek.com, Greene at adamgreene@dwt.com, Apgar at capgar@apgarandassoc.com and Kam at rick.kam@idexpertscorp.com. ✧

New Year, Old Question: 'Is Your Risk Management Plan in Place Yet?'

If covered entities (CEs) do one thing in this new year — something they should have already done long ago — it should be to *complete a risk assessment* (RA) and the corresponding risk management plan to address mitigation strategies for identified vulnerabilities. This is a task that is required of HIPAA CEs and their business associates (BAs) alike.

It's not a new refrain, but it bears repeating based on the number of financial settlements last year in which the HHS Office for Civil Rights (OCR) called out organizations for this failure. Reviewing cases that were settled will help CEs and BAs prepare for what's to come. One key is to not be a repeat offender.

"The common denominator for many of the cases in which there was a settlement was that the covered entity or business associate suffered one or more breaches affecting more than 500 individuals sometime between 2011 and 2013," says David Holtzman, who is vice president of compliance for the HIPAA consulting firm CynergisTek.

"The enforcement actions came about when investigations into the root cause of the breach found systemic, often profound, failures of organizational programs to safeguard protected health information," Holtzman says. "And most often cited was failure to perform an information security risk assessment or to have a risk

management plan to address gaps in the safeguards for information systems, both required actions under the HIPAA Security Rule."

"If you haven't performed an appropriate RA, it calls into question everything you're doing" in terms of HIPAA compliance efforts, because an RA is so foundational, says Reece Hirsch, a partner in San Francisco office of Morgan, Lewis & Bockius LLP.

OCR will want to know "how CEs have responded to their messages" in its press releases issued with each settlement and the specifics of the corrective action plans. "While this hasn't been explicitly stated by OCR, you have to figure that the industry's had a few warnings and opportunity to get their house in order," says Hirsch.

This is also the year to buckle down on other basics, including encryption, and to hone those skills at procuring the internal resources necessary to implement compliance tools.

RAs Must Address Ransomware, Clouds

OCR has made it clear that RAs must not only be thorough, they must be current. That means even if an RA was done in the last year or so, it is unlikely to address one of the newest and most dangerous threats — ransomware. In 2016, OCR issued guidance on this topic, amid a spate of high profile cases *(RPP 8/16, p. 4)*. OCR also said, for the first time, that ransomware is likely to be a reportable breach.

"I think OCR likely will continue to focus on risk analyses" in its settlement agreements, says Adam Greene, a partner with Davis Wright Tremaine in Washington, D.C, and a former OCR regulator.

The agency will continue "investigating breaches, especially large breaches, and looking at what kind of security program is in place," says Greene. OCR's recent settlements, he notes, show "they've arguably become less patient" with organizations that seem to have just conducted their first RA right after OCR contacted them.

When conducting a risk assessment, "make sure it covers all of your protected health information," says Greene, an admonition that was "as true for 2016 as it is for 2017."

The growing use of "cloud" providers is another trigger for an updated RA; this also was the topic of new OCR guidance *(RPP 11/16, p. 5)*. CEs and BAs are also increasingly deploying apps and sharing protected health information (PHI) with patients, an aspect that also must be addressed in an RA. OCR weighed in on apps in a separate guidance document *(RPP 3/16, p. 1)*.

This year "cyberthreats are not going away," says Greene. It's worth emphasizing that the security rule doesn't just mandate "confidentiality. It is also about availability" of PHI and assuring PHI can be accessed to continue offering patients services and treatment, Greene points out.

Is encryption on your "done" list or "to-do" list? This year, breaches by insiders and hackers will continue, says Greene, creating a situation where "it becomes tougher and tougher if you haven't encrypted" to justify not encrypting. Even though this is technically an "addressable" standard, OCR typically has not accepted that encryption isn't necessary.

Encryption Remains a Top Priority

In its $2.7 million July settlement with Oregon Health and Science University, for example, OCR specifically faulted OHSU for "widespread HIPAA vulnerabilities." The agency said OHSU "lacked policies and procedures to prevent, detect, contain, and correct security violations and failed to implement a mechanism to encrypt and decrypt ePHI or an equivalent alternative measure for ePHI maintained on its workstations, despite having identified this lack of encryption as a risk *(RPP 8/16, p. 1)*.

Mac McMillan, president CynergisTek, says he's advising clients "to increase their budgets right now primarily because, for the most part, we're behind in this battle with cybercrime."

CEs and BAs shouldn't neglect the basics, but they need to tailor their approaches to address current variations, says Rick Kam, president and co-founder of ID Experts, a security consulting firm and provider of credit monitoring services and, more recently, a medical identity theft protection product called MIDAS *(RPP 12/15, p. 6)*.

'Old Threats Are Back With New Twists'

"Old threats, like denial of service attacks, are back but with new twists, with hackers using massive numbers of IOT [Internet of Things] devices like DVRs and security cameras for the attack," Kam tells *RPP*. "I think the health care industry will see more of these types of attacks along with ransomware and malware attacks. This is going to require health care organizations to become proactive versus reactive in 2017."

As for where he thinks investments should go, Kam recommends "proactive forensic audit[s] looking for these types of problems versus waiting for security systems to alert them to a problem."

Getting the resources to ensure compliance involves engaging key stakeholders, something that — like the need to do an RA — might sound like a cliché but is nonetheless essential.

McMillan says he recently addressed a group of physicians at the University of Texas MDAnderson Cancer Center and reminded them what's at stake. His message

to the physicians was, "This is your business, and if you care about your productivity, if you care about the speed at which you access data, if you care about the integrity of the information that you rely on about the patients that you're touching, then you need to understand that you need to invest in the right technology and the right resources to protect that information environment so that you can have confidence in it."

Boost Internal Reporting

This year, Beth Israel Deaconess Medical Center will continue with its "three-year effort to formalize our security reporting processes," John Halamka, BIDMC chief information security officer and a widely followed health IT innovator and leader, tells *RPP*.

BIDMC uses a security information and event management product called Splunk to "track incoming attacks and our response to them. We report the number of potential infections detected, the number of breach attempts blocked, the number of phishing schemes avoided, and the number of malware infections remediated," he says. "It's important for covered entities to agree upon objective security metrics then publish these metrics on a continuous basis, presenting them to senior management as part of creating a culture of security in the organization," he adds. Sharing this data is also a way to shake funds from executives.

In addition to these internal efforts, Halamka suggests compliance officials need to help each other more. "Probably the most important thing that health care institutions can do collaboratively is share 'threat intelligence,'" he says, offering information about "who is attacking what and how."

Contact Holtzman at david.holtzman@cynergistek.com, Greene at adamgreene@dwt.com, Kam at rick.kam@idexpertscorp.com, McMillan at mac.mcmillan@cynergistek.com and Halamka at jhalamka@bidmc.harvard.edu. ✧

FDA Issues Recommendations on Medical Device Cyber-Vulnerabilities

On December 28, the FDA released recommendations for managing the cybersecurity vulnerabilities of medical devices that are connected to the Internet. The recommendations, which are addressed to manufacturers, urge attention to cybersecurity "throughout a product's lifecycle, including during the design, development, production, distribution, deployment and maintenance."

According to the FDA guidance, "a growing number of medical devices are designed to be networked to facilitate patient care. Networked medical devices, like other networked computer systems, incorporate software that may be vulnerable to cybersecurity threats. The exploitation of vulnerabilities may represent a risk to health and typically requires continual maintenance throughout the product life cycle to assure an adequate degree of protection against such exploits." To access the 30-page document, go to www.FDA.gov. ✧

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.*

◆ **Florida hospital settles data breach class action.** In December 2014, plaintiff John Doe sued the Florida Health Science Center Inc. DBA Tampa General Hospital (TGH) on behalf of himself and other TGH patients. He alleged that TGH had failed to safeguard and secure its patients' personally identifiable information (PII) and personal health information (PHI), and thereby harmed the patients when their PII and PHI were wrongfully accessed. Specifically, plaintiff alleged that in May 2014 one or more former TGH employees wrongfully accessed and obtained TGH patients' PII and PHI, including Social Security numbers, billing information, and health related information. Plaintiff further alleged that this breach was part of a series of data incidents at TGH, highlighting TGH's inadequate protection of patient information. In December 2016, TGH and plaintiff reached a settlement agreement, closing this action. In the agreement, TGH denied the allegations and did not admit any liability or wrongdoing, but agreed to settle the matter to avoid the costs and burdens associated with litigation. As part of the settlement, TGH agreed to set up a $10,000 fund to pay plaintiffs for damages and up to $7,500 to cover attorney fees and costs. To qualify for a share of the settlement, class plaintiffs must demonstrate they have suffered actual losses due to the breach. *(Doe v. Florida Health Sciences Center, Inc., 14-CA-012657 (Fla. 13th Cir. Ct. 2014)).*

Raising Employee Awareness About Cybersecurity

Piedmont Healthcare in Atlanta recently sent this notice to all employees to enlist their help in defending against cyberattacks. Contact Debi Weatherford, executive director of internal audit, at Debi.Weatherford@piedmont.org.

This message is being sent to all Piedmont employees.

…Yes YOU!

Piedmont takes information security very seriously. Because of the rise of Ransomware attacks, we need to ensure that everyone inside Piedmont understands our security expectations and what you can do to help protect not only yourself but our organization.

Online safety and security are shared responsibilities, and we each have an obligation to protect our identities and our information while online. Understand the risks, learn how to spot potential problems, and consider how your online actions can impact everyone's collective security.

Here are some tips to assist in being aware and secure:

- **Know the scams.** The Piedmont Information Security team periodically sends email nuggets about trending scams to keep you aware of how to protect yourself and our organization. In this way, you'll be armed with what you can do to avoid them.
- **Think before you click.** Never click on links in messages from people you don't know or only vaguely know. These phishing emails may have links that can lure you into giving personal information or download malware to your computer. You should even be wary with emails from people you do know if it looks or sounds suspicious. Hackers can create a malicious email that looks like it came from your manager, peer or close friend's email account.
- **Safely peruse.** Beware of phony websites. These sites may have addresses very similar to legitimate sites, and red flags may include pages with frequent misspellings, poor grammar or low resolution images. However, scammers are getting better at replicating sites. If a site asks for personal information, double check the URL and make sure it's not asking for information it shouldn't.
- **Keep it to yourself.** Don't forward suspicious email to other coworkers – it is like spreading your germs. Instead, forward the email to security.concerns@piedmont.org.
- **Shop safely.** Don't shop on a site unless it has the "https" and a padlock icon to the left or right of the URL.
- **Use common sense.** You do not need to be a seasoned computer whiz to know that it's not smart to open an attachment titled, "Claim Your Inheritance!" Using common sense while surfing the Web can protect you and Piedmont from a hungry cyber-shark.

From top leadership and executives to the newest employees, cybersecurity requires the vigilance of every employee to keep data, patients, and capital safe and secure. We can defeat cyber-criminals or at least make them look for an easier target. Thank you for your support.

OCR's Complaint Closure Letters Provide Some Interesting Guidance

What does HHS's Office for Civil Rights (OCR) say to covered entities (CEs) and business associates (BAs) when it responds to a complaint filed with the agency? OCR does not post its "closure letters," but to demystify this process, ProPublica, an independent newsroom that conducts investigative journalism, has undertaken an initiative called Policing Patient Privacy (https://www.propublica.org/series/patient-privacy). As part of this effort, it has posted 300 letters OCR sent to health care entities in response to complaints received between 2011 and 2014. ProPublica obtained the letters — a majority of which were sent to CVS and the Veterans Administration — by filing a Freedom of Information Act Request.

The letters generally respond to complaints affecting one individual, such as unauthorized use or disclosure of PHI, often by an employee, or a refusal to permit access to protected health information. By law, OCR is obligated to investigate these complaints. Upon receipt of a complaint, OCR reviews the complaint and, as necessary, requests data from the covered entity or business associate that is the subject of the complaint. It reviews the complaint and any data it has requested and makes a determination as to whether the complaint is a violation of HIPAA. If OCR finds there is no violation, it notifies the complainant and the health care entity that is the subject of the complaint. If there appears to be an issue, given time and budget constraints, those issues involving a small number of individuals generally are resolved by one of two means — technical assistance or a change achieved after voluntary compliance efforts.

Cases Resolved by Technical Assistance

According to the OCR enforcement data, in 2015 the agency resolved 22% of its cases with technical assistance. In these cases, OCR does not officially investigate the complaint but reviews the details provided by the complainant. It notifies the complainant of the technical assistance resolution and often sends a copy of the relevant regulation or a checklist of compliance procedures to both the complainant and the covered entity.

For example, in response to a complaint alleging that a CVS pharmacy did not have reasonable safeguards to prevent inadvertent disclosure of PHI because CVS employees and patients were discussing medical information within earshot of other customers, OCR sent the pharmacy a letter explaining the complaint and attached a copy of 45 CFR 164.530(c), Reasonable Safeguards. It sent a similar letter to the complainant. In another instance, a clinic faxed the patient's PHI to a wrong, unverified fax number. To resolve this complaint, OCR contacted the clinic about the complaint and mailed it a checklist of reasonable safeguards to protect against impermissible disclosures when mailing or faxing PHI.

Even violations that appear more egregious than a careless or inadvertent employee mistake may be resolved with technical assistance that puts responsibility on the entity to resolve the problem. For example, a complaint filed against Planned Parenthood alleged that an employee posted a description of the procedure the individual had performed at the clinic on the individual's public Facebook page. OCR sent Planned Parenthood the regulatory section on reasonable safeguards and encouraged it to "assess and determine whether there may have been noncompliance…and if so, to take steps to ensure such noncompliance does not occur in the future." OCR also instructed Planned Parenthood to review the case and contact the complainant with its findings as required by the privacy rule. The letter says it may conduct a compliance review in six months and, if another similar complaint is received, may conduct a full investigation.

In one of the few responses indicating no violation, OCR informed the complainant that TRICARE's release of his PHI was permissible under the HIPAA public health and safety exception (45 CFR §164.512(j)(1)). According to TRICARE, the information was disclosed because the occupational health provider determined the complainant was unfit to carry a weapon, which was necessary for his job duties. OCR did provide guidance on the release of the minimum necessary information.

Change Achieved After Voluntary Compliance

The second common path to resolution of a complaint is "Change Achieved After Voluntary Compliance Efforts." In these instances, OCR actually investigates the complaint and requests additional data from the covered entity. After receipt of the additional data, it is not uncommon for OCR to find that actions taken by covered entities in response to complaints to be sufficient to close of the case. Here are some examples:

◆ A Veterans Administration facility disclosed an individual's medicine refill request and the medical record to an unauthorized individual. After being informed of the complaint, the facility retrieved the paperwork and apologized to the individual. OCR also required it to conduct an internal investigation regarding the incident and, based on its findings, retrain staff on HIPAA use and disclosure of PHI and determine whether sanctions were appropriate. To comply with the breach notification rules, it also required the facility to conduct a risk assessment and, if necessary, report the breach to HHS; notify the complainant; document the impermissible disclosure

on the complainant's record to comply with HIPAA's accounting of disclosures requirement; and determine actions to mitigate the incident. OCR attached the regulatory provision on reasonable safeguards.

◆ A woman filed a complaint against TRICARE because her physician disclosed her PHI to her employer. She had told her employer she was concerned about a move to a new building because of allergies. The employer called her physician, who disclosed PHI regarding the issue. OCR determined this was a violation. TRICARE "counseled" the physician and required the doctor to complete remedial HIPAA training in accordance with its sanction policies.

◆ An employee had inappropriately accessed a patient's medical record, but the clinic investigated the complaint, conducted an audit of the access to the patient's medical record, and sent a letter to the complainant. These actions, in OCR's view, met its requirements to resolve the case, but it said it might conduct a compliance review of the covered entity's safeguards in six months.

◆ An ex-wife accessed the medical records of her husband's new wife and children multiple times. After an investigation confirmed the complaint, the woman was terminated and the covered entity sent a letter of apology to the complainant.

◆ An employee inappropriately accessed a patient's medical record more than 52 times. The covered entity investigated, confirmed the complaint, and terminated the employee — all sufficient actions to close the case in OCR's view.

◆ Complainant requested a credit balance on his account and received information on four other patients' accounts. He complained to the CE, which investigated the situation and determined that this was a HIPAA violation. It also performed a risk assessment to determine whether the unauthorized disclosure met the risk notification threshold and concluded that, while the disclosed data on the other patients were sufficient to potentially cause significant financial, reputational, or other harm, there was no reasonable risk because the disclosure was to one individual who brought the issue to the attention of the CE, and thus the CE did not notify the individuals. The CE also mitigated the circumstances and trained the employee and the supervisor to assure proper compliance procedures. The complainant also filed with OCR, but OCR closed the case because the CE's voluntary compliance actions met its resolution standards.

The 300 letters posted by ProPublica are just the tip of the iceberg in terms of the number of responses the agency sent out between 2011 and 2014. OCR data indicate that it resolved approximately 50,000 cases over that time period, but the letters provide interesting insight into how OCR addresses complaints and what it looks for to close a case. The OCR response time to complaints ranged from as little as a month to more than a year. ProPublica will continue to post the letters on its website — HIPAA Helper, at https://projects.propublica.org/hipaa — as it receives them. ✧

New Fact Sheet Provides Scenarios For Public Health Disclosures

Among the exceptions for the use or disclosure of protected health information (PHI) are those related to the protection of public health (45 CFR §164.512(b)(1)). As a result, covered entities may disclose PHI to public health agencies that are authorized by state or federal law to collect the information.

To help clarify these circumstances, the HHS Office for Civil Rights (OCR) and the Office of the National Coordinator for Health Information Technology issued a fact sheet on Dec. 16 with eight scenarios illustrating how these regulatory provisions work. For each scenario, the fact sheet states, three standards apply:

(1) A business associate disclosing PHI for public health must be authorized to do so in its BA agreement;

(2) If electronic PHI is disclosed, the discloser must meet the HIPAA security rule requirements; and

(3) The covered entity may rely on the public health authority's request as meeting the "minimum necessary" standard.

In its ninth scenario, the fact sheet says providers who need to share PHI with agencies or organizations for public health activities may use certified health IT to send the information to the requesting agency or organization in compliance with the HIPAA security rule.

Scenario 1: Exchange for Reporting of Disease. This scenario describes when a covered entity may disclose information to a public health authority, such as the Centers for Disease Control and Prevention, in this instance for information on the Zika virus. The CDC is acting under its statutory authority to collect disease prevention information.

Scenario 2: Exchange for Conduct of Public Health Surveillance. Here, the hospital is located in a state that maintains a central cancer registry, and state law authorizes the state's health department to collect data on cancer occurrence (including the type, extent, and location of the cancer) and the type of initial treatment.

Scenario 3: Exchange for Public Health Investigations. A school in this state has an outbreak of measles, and the state's department of health requests medical records to investigate the outbreak. It may ask all schools in the state, not just the school with the out-

break, to report confirmed diagnoses of measles, including patient identity, demographic information, and positive test results.

Scenarios 4 and 5: Exchange for Public Health Interventions. Perhaps reflecting the water supply problems in Flint, Michigan, in this scenario the state's health department implements a lead poisoning intervention program and requests lead exposure test results of children who may have been exposed. The state not only may collect the data now but may track the health and development of children over time. The department contracts with a health information exchange to collect the data from local providers.

In the second scenario, the state's public health authority is responsible for implementing a CMS-funded state innovation model to measure outcomes for patients who have both diabetes and depression and whose primary care providers (PCPs) coordinate their care. PCPs in the state may disclose the minimum necessary PHI to the public health authority to assist in the evaluation of care coordination outcomes.

Scenario 6: Exchange Subject to Food and Drug Administration Jurisdiction. A device manufacturer whose devices are subject to the jurisdiction of the FDA announces a Class I Medical Device Recall for a heart device. A physician, who implanted the device in 35 patients prior to the recall, hires a certified health IT entity to identify patients with the device. She may disclose to the FDA the PHI for these patients, including patient contact information and other health information. The physician must disclose only the minimum necessary information to support the recall, but she may seek the manufacturer's input regarding what should be disclosed.

Scenario 7: Exchange for Persons Exposed to Communicable Diseases and for Related Public Health Investigations. An individual who went to the emergency room was exposed to a communicable virus by another individual in the ER waiting room. Under local law and 45 CFR §164.512(b)(1)(iv), the hospital may use PHI and certified health IT to identify those individuals and may notify individuals of possible exposure. To investigate the outbreak of the virus, the local department of health is authorized by law to collect disease information and medical records to investigate and implement disease control measures. The local hospital may disclose the PHI of the patients exposed to the virus using certified health IT.

Scenario 8: Exchange in Support of Medical Surveillance of the Workplace. HIPAA authorizes medical surveillance in the workplace to monitor the safety of working conditions. In this scenario, a mining company hires a physician to provide health care evaluation services to the workers so the company can monitor their health. Federal and state law require the company to collect this information. The physician may disclose the workers' medical surveillance information but must provide written notice to the workers of the disclosure. As an alternative, the notice may be prominently posted at the worksite if that is where the service is provided.

Visit http://tinyurl.com/z262n7d for the text of the fact sheet. ✧

NYAG Pursues HIPAA Violation

continued from p. 1

The NYAG's office did not answer questions repeatedly emailed by *RPP*, and did not release the settlement, technically called an Assurance of Discontinuance.

The settlement joins just a handful of other HIPAA enforcement actions taken by state AGs even though officials were given the authority to bring such cases in 2009 *(RPP 11/15, p. 3)*. Still, it is the second for the New York AG alone, with another HIPAA case having been settled in December 2015 *(RPP 2/16, p. 4)*.

NYAG: 'Marketing Prohibition Was Violated'

Both Angels and AAHC are fiscal intermediaries for a New York program called Consumer Directed Personal Assistance Program. They are "responsible for paying home health care attendants to provide services to consumers" in the program.

According to the settlement, Altieri and another worker, while still employed by Angels, contacted a firm called Lifetime Assistance, described as "a HIPAA covered entity," in order to "solicit consumers to change their fiscal intermediary from Angels to AAHC." Given phone numbers, the employee contacted an unspecified number of consumers "without authorization." The Lifetime employee who provided the numbers was "subsequently terminated for violating [Lifetime's] disclosure policy," according to the settlement.

In addition to HIPAA, the actions also violated Executive Law 63 (12), which "prohibits the unlawful acts and practices in the conduct of a business," according to the NYAG.

AAHC "neither admits nor denies any of the NYAG's findings," the settlement states. The agreement was reached "to avoid the time, expense, and distraction of litigation" with the NYAG. It is still facing a civil suit brought by the owner of Angels.

NYAG Schneiderman pledged that his office "will continue to hold accountable any company that violates a patient's right to privacy, especially for commercial gain."

In his press release, he added that it is "unacceptable for a home care agency to try to pad its pockets by using patients' personal information without their consent."

According to the NYAG's press release, "AAHC unlawfully obtained Angels' consumer's phone numbers, and used the phone numbers to contact consumers to urge them to switch from Angels to AAHC. All of the consumers were already placed with Angels and did not consent to have their phone numbers used for commercial solicitations. Some patients became worried that their home health care services might be affected if they did not switch their service provider. AAHC's actions violate the Health Insurance Portability and Accountability Act of 1996 ('HIPAA') Privacy Rule."

The press statement notes that the privacy rule "gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be used for marketing. So as not to interfere with core health care functions, the Rule distinguishes marketing communications from those communications that are essential for delivery of quality health care."

'Egregious Espionage' Is Alleged

For their part, Angels officials were "hoping for jail time" and point out the settlement isn't the end of the story. But it should help with its ongoing civil suit against Altieri and seven former employees who went with him to AAHC, Angels CFO Michael Wegman tells *RPP*.

The suit was filed in Montgomery County Court in October 2015, shortly after the alleged misappropriation of files took place.

According to the suit filed by Angels and comments Wegman made to *RPP*, in 2014, Altieri and another individual offered to buy Angels but were turned down. They stipulate that, from August to October 2015, Altieri and seven other then-Angels employees secretly worked to copy patient, referral and provider files. On Oct. 13, 2015, Altieri reportedly sent an email resigning immediately, and on that same morning, Angels staff found "all our files shredded and offices cleaned out," Wegman tells *RPP*. Seven other employees, who comprised half the administrative staff, also had quit as of that morning, Wegman says.

The police were immediately called, and the NYAG became involved, says Wegman, whose father Daniel is the founder and brother Andy is the president. The family's corporation also includes an assisted living facility known as Hilton East. NYAG officials spent a week at the Angels office going over its policies and procedures while conducting the investigation into Altieri's actions, and did not find that the firm had violated HIPAA. Angels did not make a complaint to the HHS Office for Civil Rights, he says, but worked solely with the NYAG and pursued litigation on its own.

More typically, OCR enforces compliance with the federal HIPAA privacy, security and breach notification rules. In 2016, OCR inked a record 13 settlements for a total of $24.5 million in fines *(RPP 12/16, p. 1)*. However, in one recent case, OCR settled for $400,000 with the parent company of a hospital for alleged HIPAA violations, even though the hospital itself had already paid $150,000 to a state government over the same triggering incident — the loss of patient images *(RPP 10/16, p. 1)*.

Officials from NYAG "have been working on the case for over a year now," Wegman says. "We were hoping they were going to shut them down completely. The extent of their espionage and what they did was so egregious."

Civil Suit Is Still Ongoing

According to Wegman, the NYAG confirmed the allegations Angels makes in the suit against Altieri and the seven other former employees, which was filed just one week after patient and referral files disappeared. However, the NYAG settlement doesn't mention Angels.

O'Brien points out that "the confidential information referenced in the Assurance [of Discontinuance] is telephone numbers, not detailed health information as the Attorney General's press release implies. The resolution between my clients and the AG was negotiated after a full investigation by the AG's office, an investigation with which we cooperated fully."

"There are no factual allegations in the Assurance that files, computer data or other property was ever taken by All-American employees," he adds.

In All-American's response to Wegman's civil suit, the business denies nearly all of the allegations or states it does not have enough information to know if an allegation is true or false. It did admit that Altieri only gave notice he was resigning the morning he did so, but contended the other seven employees gave prior notice.

The suit also contends Altieri's gray work computer, which contained personal and confidential information about its customers, referrals and providers, among other data, is missing. Altieri left a black computer in the office, but it was not one he used for the business, according to the filing.

All-American admits in its response that Altieri did leave a black computer, but denied any knowledge about the rest of the allegations. ✧

PRIVACY BRIEFS

◆ **The "ransomware revolution" is described in *Kaspersky Security Bulletin 2016*,** which warns that one in five small or medium-sized business that paid ransom never got their data back; attacks on businesses increased threefold from January through September of this year, from one every two minutes to an attack every 40 seconds; and 62 new ransomware families made an appearance in 2016. Review the full report at http://tinyurl.com/hlduj6t.

◆ **The protected health information of 34,000 individuals was compromised when an unauthorized third party accessed an application on the network of Quest Diagnostics** of Madison, N.J., the company announced on Dec. 12. Quest notified the affected individuals, established a toll-free phone number, and is working with a leading cybersecurity firm to assist in investigating and further evaluating the company's systems. Go to http://tinyurl.com/hchy9on to access Quest's press release.

◆ **An "alarming" number of health care data breaches, 57 in total, were recorded in November 2016, with employees/insiders responsible for more than half of them,** according to the Protenus Breach Barometer, a monthly snapshot of reported or disclosed breaches impacting the health care industry. For more information, visit http://tinyurl.com/jv3prff.

◆ **HHS has issued a "Privacy Policy Snapshot Challenge" for designers, developers, and health data privacy experts to create an online Model Privacy Notice (MPN) that can help consumers learn how apps use patient health data.** "The MPN is a voluntary, openly available resource...similar to a nutrition facts label," providing a snapshot of a product's existing privacy practices, encouraging transparency and helping consumers make informed choices when selecting products. For more information, go to http://tinyurl.com/hdxye5l.

◆ **When employees are conditioned to identify and empowered to report suspicious emails, the security team's response time to breaches is reduced from an industry average of 146 days to 1.2 hours,** according to PfishMe Inc.'s *2016 Enterprise Phishing Susceptibility and Resiliency Report*. For more information, or to download the full report, visit http://tinyurl.com/hm4thsz.

◆ **The personal information of 15,000 New Hampshire DHHS clients was hacked and some of it was posted on social media in early November,** according to the *New Hampshire Union Leader.* Compromised patient data includes names, addresses, Social Security numbers and Medicaid ID numbers of clients who received state services prior to November 2015. An investigation is underway, with the chief suspect being a psychiatric patient who had access to the personal information files while working at a public computer in the library of the state's psychiatric hospital in October 2015, according to the newspaper. For more information, visit http://tinyurl.com/z7hwa3g.

◆ **Nearly one in two business executives have had ransomware attacks in the workplace and 70% of them said their company has paid to resolve the attack,** with half of those paying over $10,000 and 20% paying more than $40,000, according to an exhaustive data-rich survey from IBM Security. Access the news release at http://tinyurl.com/zms7xfd.

◆ **Cyberattacks in health care that breached the data of more than 500 patients increased 39% in 2016, to a total of 93 major attacks, up from 36 in 2015,** according to *Health Care Cyber Breach Research Report 2016,* a new study from the cybersecurity firm TrapX, Inc. Cyber attackers were responsible for 31% of all major HIPAA data breaches reported this year. For more information, visit www.TrapX.com.

◆ **Ninety-seven percent of security executives see human behavior as their greatest vulnerability,** according to the *Nuix Defending Data Report 2016.* Preventing data breaches was the top spending priority of 52% of respondents, while 42% said detection was their primary focus. For more information, visit http://tinyurl.com/gs3l3t3.

◆ **Nevada officials are investigating the online leak of personal information of nearly 12,000 individuals who applied for a medical marijuana dispensary license,** according to the *Las Vegas Review-Journal.* Compromised data included Social Security numbers, birth dates and addresses, but the data of medical marijuana cardholders was not breached, the state believes. For more information, visit http://tinyurl.com/j8mvesd.