Report on
PATIENT PRIVACY

Volume 15, Number 9 • September 2015

Practical News and Strategies for Complying With HIPAA

Contents

*There's no need to wait for your next issue to stay on top of the latest industry news! The "From the Editor" postings at your subscriber-only Web page will keep you updated all month long. Log in at **www.AISHealth.com/newsletters/reportonpatientprivacy**.*

Editor
Theresa Defino
tdefino@aishealth.com

Associate Editor
Lauren Clason

Executive Editor
Jill Brown

OCR Promises Records Access Guidance, New Website, But No Date for New Audits

Within the next month or so, the HHS Office for Civil Rights (OCR) expects to publish FAQs on patients' access to their medical records that will address details such as how much covered entities (CEs) may charge, and emphasize the requirement to provide the electronic information in the "form and format" that patients want.

Last year, *RPP* documented through a spot check of various covered entities' websites that CEs appeared to be violating requirements for fees assessed and were failing to make records available in electronic form, as required under the HITECH Act *(RPP 6/14, p. 1)*.

OCR also plans to launch a new website by the end of this year that will offer new compliance resources and be more user-friendly, according to top agency officials speaking at a recent data security conference in Washington, D.C., about a variety of new agency initiatives. They also announced news of a $750,000 settlement (see story, below).

But OCR officials were unable to provide updates of any significance about the agency's off-delayed audit program, such as whether it will even begin this year.

"We are hard at work on the next phase of the HIPAA audit program, and I know you've heard that a lot," OCR Director Jocelyn Samuels said in opening remarks at the "Safeguarding Health Information: Building Assurance through HIPAA Security" meeting, which was held Sept. 2-3. "But, it's coming and we're doing it."

continued on p. 10

Newest OCR Settlement Stems From a Familiar Problem for CEs: A Missing Laptop

If you're a HIPAA covered entity (CE) or business associate (BA) who hasn't yet learned the lesson on encrypting laptops, here's another reminder.

On Sept. 2, Jocelyn Samuels, director of the HHS Office for Civil Rights, announced her office had signed a settlement agreement with an Indiana physician group that agreed to pay $750,000 and adhere to a three-year corrective action plan.

The news came amid her remarks as the opening speaker in the 8th annual "Safeguarding Health Information: Building Assurance through HIPAA Security" meeting in Washington, D.C. (see story, above), which OCR cosponsors with the National Institutes of Standards and Technology.

OCR began investigating the 13-radiology practice, Cancer Care Group (CCG), P.C., of Indiana after it reported on Aug. 28, 2012, that a laptop had been stolen from a worker's car a month earlier. "We see that a lot, by the way, stolen lap tops," Samuels said.

According to archived news reports, the group's breach notification announcement at the time said a bag was stolen that "contained the Cancer Care Group's computer server's back-up media, which had some patient demographic information, such as name, address, date of birth, Social Security number, medical record number, insurance information and/or minimal clinical information used for billing purposes only" for

Published by Atlantic Information Services, Inc., Washington, DC • 800-521-4323 • www.AISHealth.com
An independent publication not affiliated with hospitals, government agencies, consultants or associations

55,000 current and former Cancer Care patients, according to Samuels.

CCG, which has removed the original notice from its website, did not issue a statement after the settlement was announced. In her talk, Samuels described the organization as a "good-sized, radiation oncology practice" that has 13 radiation oncologists "who serve hospitals and clinics throughout the state of Indiana."

OCR's investigation "found that, prior to this breach, Cancer Care was in widespread noncompliance with the privacy and security rules," Samuels said. "It hadn't conducted an enterprise-wide risk analysis by the time the breach occurred in July of 2012. It didn't have in place written policies and procedures governing the removal of hardware and electronic material, even though that practice regularly occurred."

The agreement, dated Aug. 31, requires Cancer Care to conduct a risk analysis within 90 days, revise and submit revised policies and procedures to OCR, and then train its workforce.

Cancer Care must provide annual reports to OCR detailing, among other things, "a summary of CCG's strategy related to the assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of e-PHI held by CCG; the identification of all outside entities assisting CCG in this process; and documentation related to the security measures CCG implemented or is implementing, if any, to sufficiently reduce the identified risks and vulnerabilities to a reasonable and appropriate level."

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

Three OCR Settlements Thus Far in 2015

This is OCR's second settlement with an Indiana covered entity and its third so far this year.

OCR's previous settlement with an Indiana CE was announced on June 24, 2015. In this case, Parkview Health System, Inc., of Fort Wayne, Ind., paid $800,000 and agreed to a one-year corrective action plan as part of an agreement involving an incident five years earlier. Parkview's plan to acquire the medical files of a physician fell apart over the condition of the records, and the system dumped 71 boxes of records containing perhaps 8,000 files on the physician's driveway *(RPP 7/14, p. 1)*.

Documents obtained by *RPP* through a review of documents opened through a Freedom of Information Act request revealed that Parkview officials never acknowledged any wrongdoing and maintained the records were not theirs and had to be returned. For her part, the physician was stuck paying for storage of the abandoned records, years after she closed her office *(RPP 12/14, p. 1)*.

OCR's first settlement this year was with a Cornell Pharmacy of Denver, which was found to have disposed of patient files in a nearby dumpster in 2012, a situation that was first reported by a television news crew. Cornell paid $125,000 and agreed to a two-year corrective action plan *(RPP 5/15, p. 1)*.

More recently, St. Elizabeth's Medical Center in Brighton, Mass., agreed to a $218,400 payment and one-year corrective action plan *(RPP 8/15, p. 1)*.

Other OCR settlements that featured laptops include:

◆ Two settlements announced April 22, 2014, collectively for $1,975,220, from Concentra Health Services following the theft of an unencrypted laptop from a physical therapy facility and QCA Health Plan, Inc. of Arkansas, which suffered the theft of a worker's laptop from a car (*RPP 5/14, p. 1*).

◆ Massachusetts Eye and Ear Infirmary paid OCR $1.5 million following the theft (and later recovery) of a laptop in South Korea, which contained PHI for 3,526 patients (*RPP 10/12, p. 1*).

◆ In December 2012, Hospice of North Idaho agreed to a settlement amount of $50,000 and a two-year corrective action plan when one of its workers experienced the loss of a laptop with data for 441 patients (*RPP 1/13, p. 1*). ✧

Proposed HHS Regulation Revises Research Protections, HIPAA

Four years after issuing an advance notice of proposed rule altering the regulations governing clinical trials, HHS and 15 other federal agencies have issued a 500-plus-page proposed rule that, if adopted, would make significant changes in how HIPAA applies to research.

HIPAA covered entities (CEs) such as medical schools and hospitals that conduct research have struggled for years since enactment of the privacy rules to mesh those protections with related informed consent and other research safeguards required under 45 CFR Part 46, also known as the Common Rule. They received some relief when the final rules implementing the HITECH Act allowed for the use of compound authorizations *(RPP 2/13, p. 1)*.

However, the new notice of proposed rule making (NPRM), scheduled to published in the Sept. 8, *Federal Register* but posted for public inspection on Sept. 2, is likely to further muddy the waters.

For example, while the NPRM would provide new categories of research that is exempt from review by institutional review boards (IRBs), "[c]ertain exempt and all non-exempt research would be required to provide privacy safeguards for biospecimens and identifiable private information."

NPRM Would Create New Exemptions

The NPRM would also exempt from the Common Rule "certain data collection and analysis activities using identifiable health information subject to the HIPAA Privacy Rule." Specifically, the NPRM mentions activities defined by HIPAA as healthcare operations, public health activities and research. This proposal is similar to provisions in the 21st Century Cures Act *(RPP 6/15, p. 8)*.

In a significant shift, the NPRM also proposes that consent and other protections be required when biospecimens are used, regardless of whether they are identifiable. This change will have "major operational implications for the functioning of the research enterprise," the NPRM acknowledges, and compliance wouldn't be required for three years after publication of a final rule.

The Secretary of HHS would also be required to develop new "privacy safeguards" that contain "standards…designed to be so that they could be readily implemented by an individual investigator, and would involve minimal cost and effort to implement."

HHS is also being asked to develop a "broad consent template" that would permit the secondary use of some research specimens.

There would be "at least two broad consent templates developed," to address specimens obtained in both research and non-research contexts. Templates will be published in draft form "at a later date," according to the NPRM. Also proposed are other changes to consent forms. For example, they would have to disclose to research participants whether their biospecimens "may be used for commercial profit and whether the subject will or will not share in this commercial profit."

In addition, organizations would no longer have the option of applying the federal standards to non-federally funded research. For those organizations with federally funded human subjects research, the NPRM extends "the scope of the policy to cover all clinical trials, regardless of funding source."

The NPRM was drafted primarily by the National Institutes of Health and the HHS Office for Human Research Protections. In a statement issued Sept. 2, OHRP officials said: "There are plans to release several webinars that will explain the changes proposed in the NPRM, and a town hall meeting is planned to be held in Washington, D.C. in October." The NPRM provides a 90-day comment period. Once finalized, the requirements would be adopted by all the HHS agencies as well as the National Science Foundation, Department of Veterans Affairs, and Department of Defense, among others.

To review the NPRM and see a summary and other related information, visit http://www.hhs.gov/ohrp/humansubjects/regulations/nprmhome.html. ✧

Ensuring Vendor Security Takes Much More Than a Questionnaire

On July 29, a patient whose protected health information (PHI) was compromised in a May data breach at Fort Wayne, Ind.-based health information exchange Medical Informatics Engineering (MIE) filed a proposed class-action lawsuit against the company, on behalf of the estimated 3.9 million potential victims. The next day, Indiana Attorney General Greg Zoeller issued a statement urging all Hoosiers to freeze their credit as the list of affected providers grew.

The incident is one of the latest cyberattacks on a health care vendor tasked with the responsibility of maintaining the security of medical records for multiple providers, and again begs the question of how covered entities (CEs) can ensure business associates (BA) are sustaining effective security measures. In many cases, CEs simply give a questionnaire to the BA, which Stephen Boyer, cofounder and chief technology officer of BitSight Technologies, says is unheard of in the financial sector, where customers are assessed by their credit score and performance over time.

continued

"You want to look at that empirical data and performance to help you drive that decision-making process," Boyer says. "Because oftentimes, if you were to just ask your organization what the problems are, they may not be sophisticated enough to know. Especially in the health care sector, you may be outsourcing legal, you may be outsourcing HR and benefits, and some of those benefits providers or law firms may not be sophisticated enough to know where their control caps are."

BitSight is a security ratings agency that publishes average ratings by industry, and also doles out individual company ratings as requested by its clients. The health care industry currently ranks second-to-last with a score of 630, just beating out education at 550. Bitsight evaluates a company's security by monitoring internal-external communications that are indicative of a cyberattack, updating its 25,000-plus company database every day as customers request evaluations of new vendors. Boyer says Bitsight has Freedom of Information Act (FOIA) requests submitted in every state, so it also catches many breaches that don't hit mainstream news.

Sample Vendor Security Questionnaire

The following are examples of questions that Lee Kim, director of privacy and security, technology solutions for Healthcare Information and Management Systems Society (HIMSS), says health care businesses should ask their vendors in determining if their security posture is up to par.

◆ How long has your company been in business? (Relatively few cloud providers have been in business for over 15 years.)

◆ Is your company independently owned, or is it a subsidiary? (Who is the true owner of the company?)

◆ Are your cloud provider/data center resources located solely in the U.S.? If they're international, which countries are they in?

◆ Do you own your data center or do you partner with a third party?

◆ How are your company's financials?

◆ Do you have a lot of health care customers?

◆ What is your uptime guarantee?

◆ Is your customer service 24/7?

◆ What is the latency and jitter on your network?

◆ What was your last significant security incident?

◆ Have you had any malicious insiders in your organization?

◆ What is the turnover rate for your employees?

◆ Are there third-party contractors that you use?

◆ Can we see the results of your latest SOC 2 report? How often do auditors conduct a SOC 2 review?

The level of spending on cybersecurity strategy is lowest in health care, he says, a fact that's evident in many of the elementary components missing from the security posture of health care entities.

It's Important to Do the Basics Well

"Oftentimes it's just missing the basic, motherhood and apple pie, what we call the blocking and tackling of security — just doing the basics well," Boyer says. "Sometimes that's hard, but a lot of times organizations feel like they have to do something super sophisticated, like threat intel sharing, when just keeping your systems updated with the latest software and patches is what you need to do to protect from most of the attacks."

When choosing a vendor, health care entities should first gauge the BA's knowledge of the industry in general, according to Travis Rosiek, chief security strategist for global governments at FireEye, Inc.

"What is their awareness of the cyber threat? To adequately and most effectively defend an organization from cyber threats, they have to understand the capabilities of adversaries and threats that are out there," Rosiek says. "How are they using that to prioritize their defensive posture or infrastructure or capabilities that they're looking to sell to these health care providers? Are they even aware of the threats or is it just a buzzword that they're using? Or do they actually understand how threats are circumventing the legacy technologies that are out there on the market? And how they are actually using that to drive their internal strategy to defend their own network, as well as harden any products or services that they're going to sell the health care provider."

Further questions are probably best answered through an on-site evaluation, although it could take time to get a complete picture of the vendor's security practice.

"Are they adequately monitoring their network and looking for advanced threat action? Are they detecting anything?" Rosiek asks, citing security operations, processes and tools that the company uses as important indicators. "Are they generating valuable data, or is it just a check-the-box kind of thing? Are they operationalizing their defensive infrastructure? Are they focused on hardening their platform? Are they doing internal security auditing or pen testing of their applications and services? Are they actually fixing things as they find them? Those are the types of things that would give you a warm and fuzzy."

Rosiek says oftentimes the easiest way into an organization is through its supply chain, and regardless of the hefty investment the company may have made in its own security, a third-party vendor with lax protocols can easily nullify those precautions. That eventually will change as the threat environment continues to evolve and the industry becomes savvier, according to Boyer.

"What we see in financial services and what will probably continue to work its way down into other sectors is the mandate for continuous monitoring," Boyer says. "It is continuous diligence and understanding the risk profile of that supply chain."

Breaking Up Isn't Easy

Ending vendor relationships can be difficult — not only in actually terminating the contract, but in determining when the relationship is no longer of any value or when the vendor's security procedures are lacking enough to warrant significant concern.

"When is the risk too high to continue the business relationship?" Boyer asks. Keeping sight of the "business value" and when that has sufficiently deteriorated is key to maintaining secure systems. "The challenge has always been for risk professionals to quantify that and to communicate that to the business, so the business can make a good case for why they may want to discontinue the relationship."

Many security organizations now have "veto rights" on certain vendor contracts, he says, and while that's mostly only in the onboarding process, it's beginning to include the duration of the contract as well. Ending the contract abruptly could be disruptive to the business, so companies should think ahead and build termination provisions into the contract ahead of time.

"You want to make sure you have some transition plan as you're transitioning away from another vendor to make sure you don't have some gap or blind spot in your organization or your security posture that an adversary can target," Rosiek says. Those aspects should be built into the statement of work and service level of the agreement.

A secure vendor has a consistent track record, both before the business relationship begins and during the relationship itself. But only continuous monitoring can keep a business apprised of its vendor's security status.

"Good performance over time does not happen by accident," Boyer says. "That usually will take vigilance. It's going to take the buy-in at the executive level, and it's going to take dedicated resources. Anybody can scramble for a couple weeks, or maybe a month's effort, but really sophisticated organizations who are dedicated to good security practices — that will oftentimes take years."

Contact Boyer via Kristina Lanpheir at kristina@kulesafaul.com and Rosiek via Kyrksen Storer at kyrksen.storer@fireeye.com. ✧

Mobile Devices Are a 'Silent Killer' Of PHI; BYOD Policies Are a Must

Mobile devices in the workplace are ubiquitous and health care organizations, more now than ever, are facing the challenge of incorporating personal devices into regular workflow as access to protected health information (PHI) expands and CMS continues its push for interoperability.

Stage three of the Electronic Health Record (EHR) Incentive Program is set to take effect in 2017, with all providers required to meet its EHR and interoperability requirements in 2018. That's a big reason for the jump in bring-your-own-device (BYOD) policies in health care, according to Ron Calhoun, health care practice leader for Aon Risk Solutions, who says that until now the industry has not been able to adapt to the trend fast enough.

"It has evolved quicker than traditional delivery systems have created policy to deal with that. What really is driving that is stage one and stage two meaningful use," Calhoun says. "Stage one and two really brought to the forefront a subset of the population that basically said 'hey, we want to be able to utilize our own mobile devices as we embark upon this journey in stage one and stage two meaningful use.' It really wasn't an issue of being sanctioned or unsanctioned; it just kind of happened."

The industry is experiencing another surge in BYOD discussions in preparing for the next step in the EHR Incentive Program, Calhoun says. "Now what we're seeing is a recent uptick again, and I think it's primarily because we're moving into stage three meaningful use," he says. "Whereas stage one and stage two really was all about digitizing paper, stage three is all about interoperability."

Calhoun thinks the interoperability movement and the value-based care movement add up to a "perfect storm" for health care providers in terms of privacy risk, because not only are they dealing with the headache of securing web-accessible clinical data, but now are dealing with the additional challenge of monitoring multiple contractors and an endless number of mobile devices.

Two-thirds of data breaches published on the HHS "Wall of Shame" are a result of lost or stolen devices, according to Rich Campagna, vice president of products and marketing for the cybersecurity firm Bitglass. In its 2015 Cloud Adoption Report, Bitglass found that adoption of cloud applications in the health care industry nearly tripled in the past year alone, from 13% to 36%.

Campagna calls lost devices the "silent killer" of health care data. While a recent survey by KPMG reported that four out of five health care firms had experienced a cyberattack (see story, p. 10), many times crooks still get the loot the old-fashioned way: through a smash-and-grab. Since there's virtually no way to ensure employees don't slip up and leave a phone on the subway, or a tablet in the passenger seat of their car, the best security is a monitoring service that allows an employer to wipe the device remotely, as Bitglass allows employers to do.

But privacy is a two-way street. With the new wave of mobile device management (MDM) or enterprise mobility management (EMM), there is what Campagna calls a more "data-centric" approach than the traditional software, which has the capability to take over a device entirely, including an employee's personal data like photos and text messages. As a result, 57% of employees are disinclined to participate in a BYOD program over privacy fears. With software like Bitglass, however, employers

Mobile Device Use Policy & Procedure

The following is an excerpt of an extensive mobile device use policy and procedure provided to *RPP* subscribers by Chris Apgar, president of Apgar & Associates, LLC, in Portland, Ore. The full policy and procedure is included at *RPP's* "From the Editor" page at http://aishealth.com/newsletters/reportonpatientprivacy. For more information, contact Apgar at capgar@apgarandassoc.com.

ORGANIZATION

SUBJECT: Mobile Device Use		DEPARTMENT:	
ORIGINAL EFFECTIVE DATE:		DATE(S) REVISED:	
APPROVED BY:	DATE:	NUMBER:	TOTAL PAGES: 5

PROCEDURE:

1. The following requirements apply to workforce members assigned a mobile device for business use:
   a. For security and supportability reasons, access to the Organization network will not be allowed using a device that is not the property of Organization or is not a personally owned device approved for business/clinical work.
   b. Workforce members with remote access will be required to use a virtual private network (VPN) connection connected to the mobile device when in use remotely.
   c. If in travel status, workforce members are required to access Organization's network using a secure connection.
   d. Access to Organization's network from a coffee shop, airport, etc. is prohibited given the risk of inappropriate disclosure of PHI related to other individual's ability to view the laptop screen displaying PHI as well as the additional security risks regarding unsecured wireless networks.
   e. Organization assigned laptops are for company business use only.
   f. If an Organization owned mobile device requires servicing, it will be the workforce member's responsibility to transport it to Organization. Remote site maintenance is not available.
   g. Workforce members' assigned mobile devices are required to securely transport the mobile device home each night and on weekends in order to ensure availability in the event of a disaster affecting Organization.

2. Mobile device assignment approval process (company-owned or personally owned):
   a. Manager approval is required.
   b. Managers are required to send any mobile device requests by email to the *[designated workforce member]* for approval. The request must indicate the equipment requested and the workforce member the device will be assigned to and business justification or that the workforce member is approved to use his or her personally owned mobile device.
   c. Workforce members who do not meet the above criteria but who believe that their assigned duties require use of a mobile device require their manager's approval. The manager will submit the request with an explanation of the unique need.
   d. Prior to assignment of an Organization owned mobile device to a workforce member or approval for a workforce member to use a personally owned device, the device will be configured by *[designated workforce member]* to comply with established portable device security requirements.
   e. Following assignment or approval, workforce members are prohibited from changing the security configuration on the mobile device.
   f. Personally owned mobile device access to Organization's network is approved in accordance with this procedure including required security configuration.

can monitor PHI from the network without installing any intrusive programs on the device itself. When employees connect to the network, or when they use work applications like email, Bitglass redirects the information to a central monitoring service before it's allowed to continue to its intended destination.

If an email with a spreadsheet of 10,000 patients comes through, for instance, Bitglass can flag that email and prevent it from being delivered. "That's probably not a work-legitimate transaction and it represents high risk of loss or breach to the organization," Campagna says. "So we'll do things like block the transaction; we can encrypt that file so that, upon receipt, we can redact out sensitive information."

Calhoun maintains that EMM in health care has increased over the past two years, and a widely cited statistic from Gartner, Inc. projects that half of all employers will require employees to supply their own devices at work by 2017. But a recent survey from secure text message provider Spok found a slight drop in the number of health care organizations that allowed some form of BYOD. In 2014, 88% of health care companies responded they did allow BYOD, while only 73% said they allowed BYOD in 2015.

Brian Edds, vice president of product strategy for Spok, says the sensitivity of PHI is part of the reason. Eighty-one percent of respondents said data security was the biggest reason for not allowing a BYOD policy. "In the general marketplace, BYOD is very easily accepted," Edds says. "But I think in health care, which is the primary target of this market, there is a lot of concern around BYOD."

In breaking down that 73%, Edds says, the survey found 90% of physicians use their own devices, while only 30% to 50% of other workforce members, such as nurses who typically share corporate-owned devices between shifts, do so. Edds also believes that because BYOD policies still are relatively new, some organizations may have responded without having a clear understanding of their own policies.

Of those companies that do allow employees to use their own devices, only half had a written BYOD policy

Mobile Device Use Policy & Procedure (continued)

3. Mobile device hard drives/flash drives used to access and store ePHI will be encrypted to guard against inappropriate ePHI access in the event the device is lost or stolen. This is also true for any portable media used with the mobile device.

   a. Workforce members shall print or download confidential information only while hooked up and logged into the Organization's network.
   b. Mobile devices actively connected to the network or information systems must not be left unattended.
   c. Mobile devices should not leave workforce members' presence when in transit.
   d. Mobile devices left in a vehicle shall not be visible. If possible, the mobile device should be stored in a locked trunk. (Weather conditions should be considered when leaving electronic equipment in a vehicle for long periods of time.) Unattended vehicles shall be locked at all times.
   e. Mobile devices, portable media and any other forms of removable storage (e.g. USB drives, CD-ROMs, flash storage cards) shall be stored in a secure location or in a locked cabinet when not in use.
   f. In a hotel, lock the mobile devices in a safe if available and the device fits.

4. Technical Support:

   a. Technology support of Organization-owned mobile devices will be equivalent to that provided for Organization owned desktop computers. Direct support will only be provided while mobile devices are at Organization sites.
   b. Should a mobile device require hardware upgrade (e.g., memory, peripheral, or hard disk), software installation, or have problems that cannot be resolved over the telephone, the mobile device will need to be brought to an Organization office for hardware service, software installation, or problem diagnosis.

5. The Organization owned mobile devices will be configured with a standard suite of programs that are appropriate for the type of device assigned based upon Organization's software standards. This includes security related configuration and software relating to personally owned mobile device use for business/clinical purposes.

   a. Other applications may be installed, based on the workforce member's needs as defined by Organization.
   b. Organization has implemented policies for appropriate use of software, including the requirement to demonstrate legal license to a program before it can be installed on an Organization-owned computer.
   c. Workforce members will not in general be given administrative rights to the Organization-owned mobile devices assigned
   d. Workforce members may not load games, entertainment software or personal finance software on Organization-owned mobile devices.
   e. Workforce members using personally owned mobile devices are prohibited from disabling or modifying security configurations and software installed to protect the security of any ePHI stored on the device.
   f. All mobile devices used to access Organization's network and IT assets must be encrypted.

*(See **RPP's** web page for this complete document)*

Web addresses cited in this issue are live links in the PDF version, which is accessible at** RPP's* ***subscriber-only page at http://aishealth.com/newsletters/reportonpatientprivacy.

in place. That's a problem, according to Edds, because it could create a "wild, wild west" atmosphere for a company's data. "No. 1, you gotta have a policy. Either allow it or disallow it, but don't stand in the middle and not say anything about it," he says. Secondly, define each role within your organization and assign a level of access. Third, identify workflows and how those devices will be used. "Allowing somebody to simply bring their phone to work and check their email is far different from using business applications that are maybe used in their workflow throughout the day," Edds says.

Barry Runyon, research vice president at Gartner, says companies shouldn't have BYOD policies in place without an EMM platform, because it can turn into a "nightmare." But that doesn't mean companies should require employees to use their own devices, either. BYOD policies should be optional, but well-incentivized and well-enforced at the same time.

"You want those that it's appropriate for and those that are willing to do it," he says. "And you incent them by paying for the service and communicating closely through upper management to the employees. But make it opt-in, because over time, that is just much more convenient."

Because there now are more mobile devices than human beings on the planet, keeping them out of the workplace is impossible, meaning a written policy is needed to regulate them clearly and effectively.

"It's not going away," Calhoun says, citing recent research by Markets and Markets, a market research company, that says EMM is increasing at a 25% annual compound rate. "It's on a pretty strong growth trajectory."

See the boxes on pp. 6-7 for excerpts of a sample BYOD policy and procedure provided to *RPP* subscribers by Chris Apgar, president of Apgar & Associates, LLC, in Portland, Ore. For more information, contact Apgar at capgar@apgarandassoc.com.

Contact Calhoun via Brin Segal at brin.segal@kemperlesnik.com, Campagna at rich@bitglass.com, Edds via Jill Asby at jill.asby@spok.com and Runyon at barry.runyon@gartner.com. ✧

Privacy/Cybersecurity Industry Faces Growing Worker Shortage

Demand is growing for health care cybersecurity professionals as hackers step up their attacks and the advent of electronic health records and the Internet of Things (IoT) increases the amount of personal information companies collect and store online. But the cybersecurity industry is still relatively new, and the demand has created a "vacuum" that is driving up salaries for cybersecurity professionals, many of whom have their pick of positions in today's environment.

PATIENT PRIVACY COURT CASE

This monthly column is written by Tamara Senikidze of Morgan, Lewis & Bockius LLP in Washington, D.C. 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 Tamara at tsenikidze@morganlewis.com.*

◆ **New York court limits the basis on which patients may sue over a security breach.** On August 14, The Queens County Supreme Court in New York held that various state and federal laws do not give a right to individual plaintiffs to sue a hospital for a security breach. The lawsuit was brought by former patients against the Nassau County hospital and its parent company, North Shore-Long Island Jewish Health System. The plaintiffs claimed that, since the fall of 2010, medical record face sheets with full names, addresses, Social Security numbers, dates of birth, medical histories and other information were stolen from the hospital. As a result, many plaintiffs have already suffered identity theft, according to the lawsuit. Among the allegations were claims for deceptive acts or practices brought under New York General Business Law (GBL) §349(h), a negligence claim based on GBL §899-aa and a claim based on an alleged violation of HIPAA. The court dismissed all but one claim, holding that the alleged violations of federal or state laws cited in the complaint did not provide for statutory or implied private rights of actions for the unauthorized release of individuals' confidential information. The judge said the plaintiffs satisfactorily pleaded one negligence claim alleging that, by providing confidential information to the hospital, the plaintiffs had an expectation that the information would be kept confidential, and therefore the plaintiffs suffered "emotional distress, mental anguish and financial damages" because their information ended up in the hands of unauthorized third parties. *(Abdale v North Shore-Long Island Jewish Health System, Slip Op 25274)*

The health care industry, with its culture of historically spending less on information security, is at a disadvantage in this competition to attract qualified cyber executives. For example, a 2013 report from the Ponemon Institute found that health care ranked last in its compensation for security professionals, with compensation cited as the No. 1 reason cyber professionals leave their employers.

Health care privacy salaries apparently mirror their cybersecurity counterparts. Sam Pfeifle, director of publications for the International Association of Privacy Professionals (IAPP), said a March survey of its health care members found that they make a median salary of $120,000, which is considerably below the privacy industry average of $152,000.

Cybersecurity Is Now in the Mainstream

Privacy and cybersecurity demand is reflected elsewhere as well. In July, the country's second cybersecurity exchange-traded fund (ETF), CIBR, debuted on the NASDAQ stock exchange, following its predecessor, the New York Stock Exchange's HACK, which passed the $1 billion mark in assets a mere eight months after its unveiling in November 2014. The series of high profile data breaches involving major companies like Target, Sony and Anthem helped drive cybersecurity into the mainstream. When Pfeifle accepted his position with IAPP two years ago, his friends and family did not understand his new job description, but that's no longer the case.

"Everybody was like, 'what's privacy? What do you mean, like a private eye?'" he recalls. "Now they know exactly what I do and they really want to talk about it."

Lisa Gallagher, vice president of technology solutions at Healthcare Information and Management Systems Society (HIMSS), says she has been encouraging her son, who just graduated from Virginia Tech with an electrical engineering degree — her degree as well — to pursue cybersecurity because, she tells him, "you'll always have a job."

"Now we have this highly visible threat environment," she says. "People hear about it every day. Organizations are starting to focus on understanding the threats and their vulnerabilities and dealing with them so they can get ahead of it if possible. I think that really accounts for the change."

Health Care Security Has Unique Complications

The number of educational programs available now is also evidence of the change, according to Gallagher, who has worked in information security for 30 years. "Until recently, there weren't curriculums offered in cyber as a specialty," she says. "There are now even master's programs. It's just all seeming to come to a point now where we're still trying to get folks who are trained and experts in this available on the market."

Earl Perkins, research vice president at Gartner, says the "acute" shortage is also a result of the multiple layers required in health care data security.

"You have a siloed style of approach, depending on the layers of security that are applied," he says. "For example, you may have a network security specialist, or you may have an application security specialist or data security specialist."

Throw in new technologies from the IoT, such as medical devices and automation, and the level of specialization deepens even further. "Most of the time we see clients that want to implement some of these modern health care systems, they go after more of a generalist, someone who understands enough about all of the different layers to be able to put together a coherent plan, and then they will go and hire a related specialist to build a project," Perkins says. "That's why you'll see that in this profession, the consulting and integration business is doing very, very well."

Medical Devices Could Pose Unique Problems

Medical devices pose a particular threat, since a cyberattack could potentially cause serious injury or death. That fear spread to the retail sector on July 21 when *WIRED* reported that researchers could remotely hack a Jeep — and drive it off the road.

"Cybersecurity as it is now, if it's done wrong, can kill people," Perkins says. "That's something I don't believe people understand fully. They think it's some kind of science fiction story."

In 10 years, however, Perkins thinks the conversation about the lack of qualified professionals will cease to exist. Health care companies currently are partnering with universities to recruit up-and-coming cyber professionals, and are also recruiting them from the military as the armed forces slim down. The vacuum will be filled because of the "premium" companies currently are offering cybersecurity professionals. Consequently, Perkins says, the conversation will evolve into something "more profound."

"Instead, we'll have a conversation about risks that particular health care organizations face and the resilience plan they have to mitigate the risks," he says. "In that regard, we're hoping to see a convergence between what you used to see in engineering, where they were focused on reliability and safety, and IT, where they were focused on confidentiality, availability and integrity of data. We're about to see a marriage of that, where you're going to see a new breed of resilience professional who knows just as much about safety — the safety of the patient, the safety of the workers — as they do about security, and we won't talk about security as a set of layers that need to be added on after you install technologies or automation or networking. Instead, it will just be assumed as part of the process."

Contact Gallagher via Kelly Wagner at kwagner@himss.org, Perkins at earl.perkins@gartner.com and Pfeifle at spfeifle@privacyassociation.com. ✧

4 Out of 5 Health Care Organizations Had Cyberattacks in Past 2 Years

More than 80% of health care executives reported their organizations were compromised by a cyberattack in the past two years alone, according to a study released Aug. 26 by KPMG LLP. Furthermore, only half of respondents felt their companies were equipped to handle future threats effectively.

Just 13% of the 223 executives polled in the *2015 KPMG Healthcare Cyber Security Survey* reported tracking once-a-day threats over the past year, which KPMG says is indicative of a lax security posture. Michael Ebert, KPMG cyber health care and life sciences leader, said in the report that these organizations are probably being compromised without their knowledge. In fact, one-quarter of respondents said they are unaware of their company's real-time capabilities to handle cyber threats.

One client saw a 1,000% increase in security threats after switching its IT security to a Security Operations Center (SOC), yet 44% of executives reported tracking between just one and 50 threats in the past year.

Vendors are another source of concern. Only 35% of executives said they have adequate resources to monitor vendor security risks. Just more than half — 55% — felt they had capable resources to handle security incidents on the whole. (See table, below.) KPMG said the majority of its survey participants increased their cybersecurity funding in the past year, but the results indicate they haven't invested enough. Eighty-six percent of providers and 88% of payers reported their organizations had indeed invested in information security, but 19% of providers and 8% of payers still did not have a designated professional solely responsible for information security.

My Organization Has Adequate Information Technology Security Resources For The Following Areas

IT compliance/risk management	70%
Managing firewalls and other critical network resources	60%
Handling security incidents	55%
Monitoring data leakage	53%
Monitoring technical infrastructure resources for health and welfare	49%
Managing vendor security risks	35%

SOURCE: *Health Care and Cyber Security*, KPMG

Payers and providers differed on what concerns them most: regulatory enforcement and litigation topped the list for providers, while it ranked fourth and third, respectively, for payers. Payers' top concerns were financial loss and reputation, while that ranked third and fourth, respectively, on the list for providers.

KPMG concluded from the survey results that many organizations need to integrate and redesign their security systems as opposed to building on top of existing platforms, which often results in inadequate controls. The firm also recommended appointing an information security specialist and partnering with an SOC to manage threats continuously throughout the day.

The survey, which was conducted for KPMG by Forbes Insights, had 56% of its responses from for-profit organizations and 44% from the not-for-profit sector. All participants had revenues of at least $500 million, with 70% reporting revenues of over $1 billion.

Access the complete survey results at http://tinyurl.com/ol6weyf. ✧

OCR Has Packed Agenda These Days

continued from p. 1

Samuels reiterated that these would be mostly "desk" audits, with some onsite, a situation that has not changed since her address at the HIPAA summit meeting in March *(RPP 4/15, p. 6)*. Samuels' comments about the audits came in a portion of her remarks in which she discussed the "awesome" projects OCR will be working on "during the next year or so."

In May, *RPP* reported that the Office of Management and Budget had approved a "survey" that will be used to identify CEs and business associates that may be audited, but was unable to confirm whether OCR had actually begun reaching out to them *(RPP 5/15, p. 11)*. Samuels said the agency had, and that OCR has also chosen a "vendor to conduct the next phase of our audit program." She did not name the vendor.

The first phase, conducted by KPMG, Inc. *(RPP 5/12, p. 1)*, showed widespread noncompliance among CEs of all sizes *(RPP 3/13, p. 1)*. The second phase of the audits, which was scheduled to begin in 2014, marks the first time business associates (BAs) are to be included *(RPP 10/14, p. 1)*.

Samuels announced during her talk that OCR is working on medical records access guidance. During her presentation the following day of the conference, Deven McGraw, deputy director for health information privacy, discussed this topic in more detail, including stating that the guidance would take the format of FAQs so it can more readily be updated.

Samuels discussed patient records guidance in the context of OCR's part in developing a privacy framework for the White House's new precision medicine research program. The guidance will remind patients of their rights and CEs of their obligations, she said, noting that HIPAA requires CEs to give patients access to their own records, but also to share that information with third parties when requested.

Patient access, however, is not a new topic for OCR.

In 2013, OCR launched a public awareness campaign, "Information is Powerful Medicine," and then-OCR Director Leon Rodriguez, in the same year, issued a rare letter to patients informing them of their rights to access their medical records *(RPP 6/13, p. 1)*.

McGraw was speaking for the first time since joining OCR *(RPP 7/15, p. 7)*. In her remarks, she emphasized that her priorities will be outreach, education, guidance and enforcement — in that order. Referring to the medical records guidance, McGraw said she thought this would be released by the end of October.

Ensuring patients' access was a priority of hers before she joined OCR, which meshed with what OCR was already working on, she added. Regarding fees, OCR is working on how CEs can calculate the costs when the data are electronic, as current methods in use today are based on page counts. In addition to fees, the FAQs will address what constitutes a designated medical records set and what the role of BAs are in sharing patient data.

In somewhat surprising remarks, McGraw said CEs can send records information to patients in an "unsecure way" if that is what they want, as this would be in literal compliance with the format provisions in the HITECH Act.

Other Projects Are Underway

Other topics Samuels addressed during her wide-ranging talk include the following:

New OCR website is coming. Samuels said she hoped that by December OCR will have launched an updated website that will provide improved searches and access to guidance and other documents that are more user-friendly.

Breach reporting continues apace. In the six years since the breach notification rule went into effect, OCR has received "over 1,300" reports of "large" breaches, those affecting 500 or more people. According to information provided by Iliana Peters, OCR senior advisor for HIPAA compliance, there were more then 179,000 small breaches. Although the latter number is large, Samuels said the "silver lining" is that "most are indeed very small," often affecting one or two people.

Hacks account for 9% of reported large breaches. Even so, these recent breaches have affected "tens of millions" of Americans, Samuels said.

Investigations are underway. OCR investigates all large breaches and Samuels indicated "we are investigating those breaches that have been reported. I can't provide you details on those investigations because they are currently ongoing."

PHI heading out your door needs attention. In addition to the usual admonitions to CEs about risk assessments and the use of encryption, Samuels said covered entities should "have processes in place to know what information is leaving their networks, and in particular, what's happening with large packets of information that move over firewalls."

"Portal" to probe security of emerging technology. OCR is interested in hearing from developers of new health care applications and tools, and plans to develop a "portal" so they can send queries to OCR about the applicability of HIPAA, Samuels said. Although it wasn't clear how this would work, the discussion would be "interactive" and provide a "public dialogue," said Samuels, and she promised OCR would share the responses it develops.

Older Projects Were Not Addressed

Samuels did not mention the status of breach notification, minimum necessary or any of the long-awaited guidance documents OCR has been working on. Neither Samuels nor McGraw provided any details on the cloud guidance.

Peters, the third OCR speaker at the conference, gave an overview of OCR's responsibilities and duties and described basic CE compliance tasks, such as breach notification.

None of the OCR speakers addressed any of the regulations that are in development, such as the proposed rule to address providers' roadblocks to contributions to the National Instant Criminal Background Check System (NICS). OCR published an advance notice of proposed rulemaking two years ago in response to the mass murders at Sandy Hook Elementary School *(RPP 5/13, p. 1)*. A follow-up proposed rule has been under review by the Office of Management and Budget since January of this year *(RPP 4/15, p. 7)*.

Presentations from the NIST meeting, and an archive of the event when available, can be found at https://tinyurl.com/pw2vkel. ✧

PRIVACY BRIEFS

◆ **UCLA Health on Sept. 1 notified its patients of another data breach, the third mishandling of protected health information (PHI) in as many months, after an employee's laptop was stolen from his car in July.** The laptop contained names, dates of birth, phone numbers, email addresses, dates of treatment, medical record numbers and other medical information. That same month, UCLA notified patients of a cyberattack potentially affecting 4.5 million people, subsequently mailing notification letters to the wrong recipients. The new breach occurred just before UCLA defeated a previous breach victim's $1.25 million lawsuit in court on Sept. 3, after a temporary employee unlawfully accessed and shared her medical records in 2012. UCLA also faces a proposed class-action lawsuit over the July cyberattack. Visit http://tinyurl.com/ng849ba.

◆ **Akron Children's Hospital on Aug. 25 notified more than 7,600 patient families that it had lost a back-up hard drive containing voice recordings between emergency dispatchers and medical staff.** The recordings were taken during calls before or while transporting patients to its medical facilities. The hospital said staff typically only used age and gender in referring to patients during transportation, but occasionally used names and other identifying information. Akron said an internal investigation determined that the hard drive was merely lost, not stolen. Visit http://tinyurl.com/pbnbxoj.

◆ **There have been 185 health care data breaches so far this year,** according to Sept. 1 data from the Identity Theft Resource Center (IDTRC). That number accounts for 78% of all breached records — nearly 110 million — and comprises 35% of all data breaches in 2015. The IDTRC updates its data breach figures weekly. For more information, visit http://tinyurl.com/pyfcsbl.

◆ **The U.S. Attorney's Office in northern Illinois on Aug. 24 indicted a Chicago woman for allegedly filing false tax returns, including those under the names of some nursing home patients.** The indictment did not detail how Shantell Winters allegedly obtained the information, but said the scheme ran from late 2009 or early 2010 until the middle of 2012. Winters was charged with 12 counts of wire fraud, three counts of identity fraud and one count of filing a false claim against the United States. Visit http://tinyurl.com/nfeksyc.

◆ **The Colorado Dept. of Health Care Policy and Financing said on Aug. 17 that, between May and July of this year, it had inadvertently mailed out letters containing PHI to the wrong recipients of 1,622 households.** The error was corrected on July 5, when one individual who received a letter notified the department. In most cases, only one person received an incorrect letter, but in some cases as many as three people received them. Compromised data included names, addresses, state ID or Medicaid numbers, family member and employer names, income information, subsidy amounts and the person's Medicaid or Child Health Plan Plus status. The department said it was taking steps to retrieve the letters. Visit http://tinyurl.com/pqtjjz9.

◆ **A Boynton Beach, Fla., hospital employee was arrested and charged with stealing her coworkers' identities to shop and pay bills,** the *Sun Sentinel* reported on Aug. 10. The woman allegedly used 20 different identities to make approximately $20,000 worth of charges, including a $1,160 purchase at Nordstrom, after creating a fake driver's license with Keira Knightley's photo to open accounts. Visit http://tinyurl.com/qce7gt9.

◆ **A victim of tax refund fraud on Aug. 4 sued Delaware-based health care payment processor Intermedix Corp. for failing to protect his information after an employee sold it for profit.** The proposed class-action lawsuit, filed in the U.S. District Court for the Southern District of Florida, alleges Intermedix failed to properly notify affected individuals of the data breach stemming from a four-month period in 2012 when an employee was stealing sensitive information of individuals who used emergency medical services tied to the company. Visit http://tinyurl.com/pt32udb.

◆ **Massachusetts-based medical group Prima CARE, P.C. recently notified patients that two binders containing PHI were found in the bushes at a parking lot in June.** A former employee had made the binders to track work performance. The binders contained names, dates of birth, addresses, phone numbers, medical record numbers, hospital account numbers, insurance numbers, treatment dates and other clinical information for patients treated between 2007 and 2012. Prima CARE said one patient's full Social Security number also was included. Visit http://tinyurl.com/osnqjl4.