Report on
Patient Privacy

Volume 18, Number 3 • March 2018

Practical News and Strategies for Complying With HIPAA

Contents

HCCA

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

Senior Writer
Jane Anderson

Copy Editor
Bill Anholzer
bill.anholzer@hcca-info.org

(Almost) Everything You've Always Wanted to Know About Blockchain But Were Afraid to Ask

Blockchain is among the innovations that are expected to catch on in health care. But leaders at many HIPAA covered entities (CEs) and business associates are understandably confused about the term and might not feel confident engaging in even superficial discussions about blockchain with their privacy and security colleagues. This is understandable, with ransomware, breaches, mobile devices and emerging cybersecurity threats to keep them up at night.

To help introduce blockchain to privacy and security officers, *RPP* spoke to Anh Ngo, MD, a board certified anesthesiologist who is an expert on blockchain as well as on Bitcoin, the first and best known manifestation of blockchain.

Ngo (pronounced "no,") is a big believer in blockchain for its potential to "disrupt" health care. (He's also the sort of person who uses disrupt as a positive term and he previously "mined" for Bitcoin). He is a peer reviewer for a new online, open access journal, *Blockchain in HealthCare Today* (see https://tinyurl.com/yamu36wg).

Ngo, who describes himself as "not your typical physician," tells *RPP* blockchain may be most useful for billing and ordering, but it also could provide significant benefits in speeding up the secure exchange of protected health information (PHI) between patients and providers. No doubt there are also challenges to adoption, says Ngo, including how implementation of blockchain will be regulated.

continued on p. 10

'All of Us' Study Set to Launch Soon; Massive Project Will Test Privacy, Security Safeguards

Within the next four years, the National Institutes of Health (NIH) hopes to enroll up to 1 million people in its landmark research program called All of Us. But whether the program meets that goal may depend in large measure on participants' confidence in the security of their protected health information (PHI). To ensure success, All of Us has imposed perhaps unparalleled levels of safeguards and requirements, including 30-day notification in the event of a breach.

All of Us is the new name for an initiative that began under former President Obama called the Precision Medicine Initiative. The HHS Office for Civil Rights (OCR) helped develop the privacy framework that underpins the program, and issued related guidance on patients' access to their medical records. OCR also enforces compliance with the HIPAA privacy, security and breach notification rules. Last month OCR announced its second settlement of the year, $100,000 with a now-defunct document storage and shredding organization (see story, p. 4).

In the fall, NIH began a controlled enrollment in the program. As of February 23, All of Us had more than 16,000 "full" participants who had not only consented to be part of the study but had completed all portions of the protocol, Katie Rush, All of Us spokeswoman, tells *RPP*.

continued

All of Us is set to launch its national enrollment campaign this spring. "We're in the process of finalizing our date for the announcement," Rush says. NIH Director Francis Collins recently told *The Washington Post* the goal is to reach 1 million participants by 2022.

Currently the program has more than 90 "awardees/subawardees in our consortium that support various aspects of the program, from outreach and enrollment to data collection and storage," she says.

Eric Dishman, All of Us director, explained at a recent meeting of the program's advisory panel that the rollout will be "grass-roots" and accompanied by "broad-based invitations," health fairs and similar events. "At that point, we'll unleash…the formal relationships that we have with both the community partners that we've announced."

However, what exactly will be studied is itself under study. Last month, researchers and others submitted ideas, and the program will hold a closed "research priorities workshop" March 21-23 in Bethesda, Maryland, "to identify key research priorities and requirements (such as data types and methods) for future versions of the All of Us protocol."

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, hcca-info.org.

Editor: Theresa Defino

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

To order an annual subscription to **Report on Patient Privacy** ($554 bill me; $524 prepaid), call 800.521.4323 (major credit cards accepted) or order online at hcca-info.org.

Subscribers to this newsletter can receive 12 non-live Continuing Education Units (CEUs) per year toward certification by the Compliance Certification Board (CCB)®. Contact CCB at 888.580.8373.

Perhaps in spring 2019, All of Us will open a portal just for researchers.

The program has been enrolling 200 to 300 participants a day, with a goal of 1,200 per day to reach the 1 million target, Dishman said.

The biobank, which is housed at Mayo Clinic, now holds 350,000 "of what we hope will be 34 million vials," according to Dishman. He said "each person's samples get broken up into multiple tubes [and] stored at multiple locations because you wouldn't want your freezers to go down in one spot to wipe out this precious resource that people have so kindly donated to us."

Additionally, "different scientific studies need tubes arranged in different ways for different kinds of research questions that are there," Dishman said.

In addition to Mayo, a number of academic medical centers are already involved. Vanderbilt University was selected as the primary data and research center; it is working with the Broad Institute and Verily Life Sciences, a subsidiary of Alphabet, the parent company of Google.

Research Focus Still Uncertain

Columbia University Medical Center, Northwestern University Feinberg School of Medicine, and the University of Texas Health Science Center at Houston School of Biomedical Informatics are also serving as data and research centers.

All of Us began a "closed" enrollment phase last summer, under which participants were invited to join and had to apply their special "code" to enter the study.

Under the initial study protocol, participants who have given their consent to be part of the study are asked to complete three health surveys, permit access to the electronic health record, have their body measurements taken and give blood and urine samples. As the program matures, other surveys now in development will be added.

According to Dishman, All of Us is not seeking to build a "disease-oriented cohort per se, but [is] focusing on those who have a wide range of conditions at [the] start and many people who are healthy so we can actually see how the absence or presence of health unfolds over time." The program is also seeking "as rich of a diversity of data as we can, to collect environmental, behavioral, social and clinical data," he said.

All of Us promises to be a landmark program for a number of reasons besides the 1 million enrollees, who are referred to not as research subjects but participants. In addition, the program has its own lingo: people who enroll on their own are called direct volunteers, or DVs; medical systems involved both in management and recruitment are known as health provider organizations, or HPOs. Answers to surveys used in the study

completed by participants are called participant provided information (PPI).

All of the data is encrypted, and the program segregates "identifying information separate from" PHI. For more details, see https://www.joinallofus.org/privacy-safeguards.

Chris Lunt, the chief technology officer, provided *RPP* additional specifics on the program's data security safeguards.

"All of Us uses the most up-to-date industry standards and practices to prevent security breaches," Lunt says. "We have enlisted teams of experts to establish safeguards and conduct rigorous security testing on an ongoing basis. These experts make sure our security practices meet the program's requirements and all federal, state, and local laws and regulations for safeguarding participant data."

The program also follows a "risk management framework comprising the National Institute of Standards and Technology guidelines coupled with our FISMA [Federal Information Security Management Act] rating to meet the program's operational security needs," Lunt tells *RPP*.

According to information provided to *RPP*, to further ensure the privacy and security of the data, the program:

◆ removes "names and other direct identifiers from participant information and replace them with a code. The codes and names are linked on a master list, kept securely and accessible to very few people."

◆ stores participants' personally identifiably information "at enrollment and data collection sites, the All of Us Data and Research Center, and the All of Us Participant Technology Systems Center. All of the data is encrypted and stored securely on protected computers."

◆ limits and tracks "who sees the information."

◆ gives participants the option to "choose which information they want to share with All of Us. Some information will be visible to the public. However, this information will be combined with information from many other people, so it won't show details about individual participants. Their names and other direct identifiers will not appear."

◆ will notify participants of a security breach within 30 days "if there is a risk to participants' privacy."

◆ requires researchers to "prove who they are" before seeing individual participants' data as well as complete ethics training.

◆ prohibits researchers from contacting or identifying a participant and

◆ will "carefully" vet requests for participants' biosamples on a "case-by-case basis by a special committee" with members to include "scientists and members of the public. Information about the studies that use All of Us samples will be available on our website."

The program also provided to RPP excerpts from the "interconnectivity security agreement" between the Data and Research Center and partner organizations.

PATIENT PRIVACY COURT CASE

This monthly column is written by Ellie F. Chapman 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 Ellie at ellie.chapman@morganlewis.com.*

◆ **Lawsuit Alleges Michigan is Unlawfully Storing Newborns' Blood.** On February 8, a group of Michigan parents sued the state's Department of Health and Human Services ("Health Department") over the collection and indefinite retention of blood samples taken from their children as newborns. *Kanuszewski v. Michigan Department of Health and Human Services et al., No. 1:18-cv-10472* (E.D. Mich. Feb. 8, 2018). The program, run by the Health Department, requires healthcare professionals who care for newborns to collect blood samples within the first 48 hours of newborns' lives to test for more than 50 maladies, disorders and diseases. The program has collected and stored approximately five million blood samples to date. In their complaint, the plaintiffs describe the practice as a "noble public policy idea" but allege that the practice is being done without parents' knowledge or consent and violates constitutional rights under the Fourth Amendment. The plaintiffs also allege concern about the potential for misuse and the "possibility of discrimination against their infants and perhaps even relatives through the use of such blood samples and research activity." According to the complaint, this concern is particularly troublesome, given that there currently do not appear to be any legal restrictions to limit who can access and use the blood samples. In addition to damages, the suit seeks an order declaring the conduct of the defendants to be unconstitutional, and requests that the practice be halted and all data be destroyed and the blood samples returned to their parents. Similar lawsuits have previously been initiated with varying degrees of success in Indiana, Minnesota and Texas.

The partners must comply with the following terms, which include:

◆ "Technical safeguards include mandatory full-disk encryption for all DRC system connected workstations, which are centrally managed to ensure that they receive the most current anti-virus and malware protection.

◆ The workstations are connected via a network that is designed to isolate network traffic containing sensitive information (such as PHI and PII) and only [*partner organization*] controlled devices can be on the isolated network.

◆ The network is protected via firewalls and network intrusion devices. All devices on the [*partner organization*] network are routinely scanned to ensure that they are current with the latest security patches and anti-virus and anti-malware updates.

◆ This is supplemented by periodic penetration tests conducted by both [*partner organization*] staff and external security vendors. A 24x7 Security Operations Center monitors the [*partner organization*] network for evidence of malicious activity and notifies an Incident Response Team as warranted."

A version of this article appeared in the February issue of *RPP*'s sister publication, *Report on Research Compliance.* For more information or to order, visit https://tinyurl.com/ybckdbd7. ✧

'Zombie' Records Storage Company Nets OCR $100K in New Settlement

In another example of the federal government exacting a toll on an organization already sanctioned by state authorities, the HHS Office for Civil Rights (OCR) recently collected $100,000 from a defunct medical records document storage company in Illinois. FileFax, Inc., paid the state $30,000 in 2015 to settle allegations that it had violated HIPAA and state laws for the same document-dumping incident that led to the Feb. 13 OCR announcement.

A bit of a zombie firm, FileFax, founded in 2000, was itself in receivership by the time OCR concluded its investigation and announced the agreement for payment and corrective action plan (CAP) that calls for proof of cataloging and proper disposal of the records.

The settlement also demonstrates the ripple effect of what seemed like a woman's innocent attempt to earn a few dollars by attempting to turn the discarded documents she found unsecured in a Dumpster into cash at a shredding/recycling company. Unfortunately for FileFax and its former clients, the owner of the shredding firm recognized the 1,100 pounds of paper as medical records from a local pulmonary practice and blew the proverbial whistle. Under HIPAA, old, discarded or unusable records must be stored and/or disposed of through secure means.

FileFax's actions caused Suburban Lung Associates to have to go through the breach notification and mitigation process, but the practice wasn't subject to any formal enforcement actions. However, a group of pediatric gastroenterologists wasn't so fortunate—and, of course, neither was FileFax.

Illinois initiated its case against FileFax in May 2015 and settled it that October. According to records the state provided to *RPP*, the woman asked for, and received, permission from FileFax to take the documents.

As part of its settlement with the state, FileFax had to name its clients and among them was the Center for Children's Digestive Health (CCDH). Although the state appears not to have pursued CCDH, OCR concluded CCDH didn't have the required business associate agreement (BAA) with FileFax, a HIPAA violation.

CCDH settled with OCR for $30,000 in April of last year. Without admitting any wrong-doing, CCDH also agreed to follow a three-year CAP *(RPP 5/17, p. 1)*.

Business Was Disolved

In its new agreement with FileFax, OCR revealed that the woman who had the records, which were for 2,150 individuals, brought them to The Shred Spot on three different days in February 2015. News reports at the time also indicate that a television station found FileFax records.

OCR accused FileFax of impermissible disclosure of the records. Interestingly, it did not allege the firm violated any other HIPAA requirements, such as a failure to have a BAA.

The state required FileFax to adhere to a number of practices if it remained in business, or to return the information to clients or otherwise properly dispose of it if it closed shop. In 2017, *RPP* found the phone number for the firm was disconnected and that it had been the subject of a three-day online auction in January of last year.

According to the OCR agreement, an attorney named Sandor Mark Jacobson was appointed the receiver for FileFax in November 2016. He accepted the OCR settlement on behalf of FileFax and agreed to fulfill its requirements, most of which had a deadline of a week from the date the OCR agreement was signed. No dates or signatures appear on the documents OCR released, but agreements are generally not made public until they have been signed by all parties. The agreement also indicates that FileFax "was involuntarily dissolved by the Illinois Secretary of State" on Aug. 11, 2017.

In most settlements, CAPs outline steps that will bring the errant organization into compliance and can serve as a template for others. In this instance, the

CAP provides direction to those dealing with the aftermath of a failed business and its trail of discarded medical records.

Jacobson, according to the settlement, had some FileFax records moved from FileFax's office to a facility operated by Iron Mountain Information Management, LLC. The CAP also required Jacobson to provide OCR "an affidavit, signed under oath, detailing where and when" he or a representative found "remaining medical records."

OCR Seeks Proof of Disposal

The affidavit was also to describe "the steps taken after their discovery to secure them, including their transference to Iron Mountain" and "the process undertaken to catalogue the records." Jacobson was also required to "formulate a plan to dispose" of the records and submit it to OCR for approval, after which he was to "seek authorization from the Court that appointed him the Receiver of Filefax…to implement the Records Disposition Plan."

Lastly, after "final disposal of all Remaining Medical Records, the Receiver shall attest that all PHI in its possession was properly disposed of as outlined in the Records Disposition Plan," the OCR agreement states.

The OCR documents list Chester Foster, Jr., of Foster Legal Services, PLLC, as the "authorized representative and contact person regarding the implementation of this CAP and for receipt and submission of notifications."

RPP contacted both Jacobson and Foster for comment on the settlement, and inquired as to whether the payment had been made and the status of the records. "Neither the Receiver nor I wish to comment on this matter," Foster told *RPP* in a response emailed on March 1.

This is OCR's second settlement of 2018. Its first was for $3.5 million with Fresenius Medical Care North America, announced on Feb. 1 *(RPP 2/18, p. 1)*. Coincidentally, while Fresenius is not in receivership, it is going through a bankruptcy reorganization.

The agreement with FileFax echoes a 2016 settlement that OCR had with a hospital in Rhode Island that lost X-rays. In 2012 Women & Infants Hospital, based in Providence, lost an unencrypted backup tape with images and data for 14,040 patients. OCR said the hospital was a covered entity and that the parent firm, Care New England, was its BA.

Women & Infants paid $150,000 to the commonwealth following the loss. However, the only alleged failure described in OCR's $400,000 settlement agreement was that Women & Infants "impermissibly disclosed" protected health information to Care New England because it failed to update the BAA it had with its parent company *(RPP 10/16, p. 1)*.

See the settlement at https://tinyurl.com/y8a8j4lh. ✧

OCR Writing New Rules Governing NPPs, Provider-Family Discussions

Providers who hate having to deal with notices of privacy practices (NPPs) and who feel stymied when talking to patients' families may soon be getting relief. The HHS Office for Civil Rights (OCR) is drafting two separate notices of proposed rule-making (NPRMs) that would alter requirements under existing rules governing these two basic HIPAA-related activities.

Information about OCR's efforts is found in a governmentwide listing of regulations under development called the Unified Agenda and Regulatory Plan. Typically updated twice a year, the Trump administration posted its first agenda, marked Fall, in December.

According to the unified agenda, which is posted on reginfo.gov, "The propsed (sic) rule would change the requirement that health care providers make a good faith effort to obtain from individuals a written acknowledgment of receipt of the provider's notice of privacy practices, and if not obtained, to document its good faith efforts and the reason the acknowledgment was not obtained."

The agency provided no additional information online about how the requirement would be changed. In response to *RPP*'s request for clarification, OCR said it could not comment on agenda items. According to reginfo.gov, the NPRM is expected to be published in September.

NPPs typically run several pages long and the obligations related to them are many.

NPPs Required Since Day One

For the past 15 years—ever since it went into effect—the privacy rule has required "health plans and covered health care providers to develop and distribute a notice that provides a clear, user friendly explanation of individuals rights with respect to their personal health information and the privacy practices of health plans and health care providers."

As OCR explains on its website, "The notice is intended to focus individuals on privacy issues and concerns, and to prompt them to have discussions with their health plans and health care providers and exercise their rights." The NPP also contains information on how a complaint about a possible HIPAA violation can be made to the covered entity (CE) and to OCR. The agency has provided a number of sample or template NPPs for CEs to use.

CEs are required to give individuals an NPP "no later than the date of first service delivery…and, except in an emergency treatment situation, make a good faith effort to obtain the individual's written acknowledgment of receipt of the notice." Typically providers have a

separate signature sheet attached to the NPP for the individual to sign acknowledging receipt.

But the 2003 rule also outlines the provider's obligation if the "acknowledgment cannot be obtained." In this case, "the provider must document his or her efforts to obtain the acknowledgment and the reason why it was not obtained." This is the language that is referenced in the regulatory plan as being subject to change under a forthcoming NPRM.

NPPs also must be updated and redistributed within 60 days of any "material revision." In 2013, all CEs were required to revise and reissue their NPPs to inform patients about new rights under the HITECH Act and to highlight when patient authorization is required before sharing protected health information *(RPP 9/13, p. 5).*

Anyone who requests an NPP can get a copy, and the CE "must prominently post and make available its notice on any web site it maintains that provides information about its customer services or benefits."

Although a foundational and long-standing requirement, compliance with the NPP mandate has been a weak spot among CEs as evidenced by the results of OCR audits. During the first audit phase, which was from 2011-2012, OCR contractors reviewed a total of 115 CEs and made 979 "findings and observations" for privacy, security and breach notification requirements.

While the largest portion (44%) of privacy related findings stemmed from uses and disclosures, 20% related to NPPs. Lack of knowledge was cited as the reason for 29% of the privacy-related findings *(RPP 3/13, p. 1).* OCR is currently engaged in a follow-up audit program *(RPP 4/16, p. 1).*

Sharing in the Patient's Interest

OCR provided somewhat more information about the second NPRM it is drafting, titled "HIPAA Privacy Rule: Presumption of Good Faith of Health Care Providers." The expected publication month is May.

"The proposed rule would modify the HIPAA Privacy Rule to clarify that healthcare providers are presumed to be acting in the individual's best interests when they share information with an incapacitated patient's family members unless there is evidence that a provider acted in bad faith," the reginfo.gov entry states.

"OCR currently defers to a healthcare provider's professional judgment in these circumstances and has never taken enforcement action against a healthcare provider who shared information in good faith," it says. That won't change. The proposed rule will not "significantly alter HIPAA enforcement policy," according to the description.

Further, OCR says the change "will not decrease the privacy protections for individuals' protected health information."

This NPRM is the third fairly recent action OCR has taken related to efforts the government is taking to address the opioid epidemic. In October, OCR issued guidance on how CEs may share information with friends and family members of those treated for opioid abuse, part of a national response to a growing crisis *(RPP 11/17, p. 1).* OCR also published "Communicating with a Patient's Family, Friends, or Others Involved in the Patient's Care" *(RPP 9/17, p. 1).*

Both proposed rules are described as "deregulatory" actions. The Trump administration has pledged to roll back burdensome regulations and required agencies to identify two rules to be withdrawn for every new one proposed. It is not evident from the reginfo.gov information on the NPRMs if any particular rules are marked for withdrawal.

The NPP proposed rule is designated as "major" and "economically significant," which is defined as one that "has resulted in or is likely to result in (1) an annual effect on the economy of $100 million or more; (2) a major increase in costs or prices for consumers, individual industries, federal, state, or local government agencies, or geographic regions; or (3) significant adverse effects on competition, employment, investment, productivity, or innovation, or on the ability of United States-based enterprises to compete with foreign-based enterprises in domestic and export markets."

The government accepts comments on NPRMs before publishing final rules. Any new requirements likely would not go into effect for several months or up to a year after a final rule is issued. ✧

Aetna, Triple-S Breaches Show Need To Pay More Attention to Mailings

Recent breaches involving mailings underscore the importance of having business associate agreements (BAAs) in place for mailing vendors, plus stringent quality control on all mailings regardless of whether they're produced in-house or by a contractor, HIPAA attorneys say.

Two recent widely-publicized breaches—Aetna, Inc.'s mailing that disclosed the use of HIV medications (*RPP* 2/18, p. 5) and a mailing from Triple-S Management Corp. that went to the wrong addresses—show that the process of sending protected health information via the postal service has many moving parts where privacy breaches can occur.

"Although the Aetna and Triple-S incidents are pretty different, they both demonstrate that even as cyber-incidents grab most of the headlines when it

comes to data breaches, paper-based mailings present plenty of opportunities for error and can be a potent source of risk for covered entities and BAs," says Alex Pearce, attorney with Ellis & Winters LLP in Raleigh, N.C.

Meanwhile, there were at least two other breaches involving mailings in late 2017 and early 2018, including one that involved window envelopes.

◆ A vendor for Tufts Health Plan that mailed member identification cards to 70,320 Tufts Medicare Advantage members used envelopes that showed the Tufts Health Plan member ID number, in addition to the member's name and address.

According to the breach notification posted on Tufts' website: "The member ID number is not supposed to be visible in the address window of the envelope." The mailing took place between Dec. 11 and Jan. 2, and Tufts says it discovered "the full extend of this error" on Jan. 18. The health plan states: "We have consulted with experts in the legal and fraud areas, and we have determined that this situation presents a very low risk to any member's personal information."

◆ A series of programming and printing errors at CarePlus Health Plans, a Medicare Advantage insurer in Florida, resulted in explanation of benefits (EOB) letters for some members being incorrectly sent to other members. This breach potentially affected around 11,200 individuals. The information disclosed included names, health plan identification numbers, dates of service, provider names, and services provided.

CarePlus says it is taking additional steps to protect privacy as a result of this incident, including "enhancements to our printing software to prevent formatting errors, more rigorous testing procedures and implementation of additional quality audit controls of EOBs prior to mailing."

In the Aetna case, Aetna agreed in January to pay $17 million to settle a federal class action lawsuit from affected members, and now is sparring in court with two vendors that were involved in the mailing.

Papers filed in support of the settlement allege that Aetna improperly transmitted to its legal counsel and a mail vendor the names of 13,487 customers who had been prescribed HIV medications, and that large, transparent window envelopes revealing confidential HIV-related information were sent to 11,875 of them.

Meanwhile, Triple-S of Puerto Rico reported that the protected health information of 36,305 plan members may have been disclosed when notices from a November 2017 mailing intended for providers were sent to the wrong addresses. The company says it performed "an extensive investigation" and has taken steps to correct its mailing process. Triple-S had previously paid OCR $3.5 million in 2015 following a series of HIPAA breaches from 2010 to August 2015 (*RPP* 12/15, p. 1).

Pearce notes that Triple-S Management's report to OCR indicates that there was no business associate involved in the mailing, so the breach may have originated in-house.

"The company's notice to its members says that notices sent to health care providers involved in the treatment of its members were mailed to the wrong addresses, but it doesn't say how exactly that happened," he says. "The company says that among the steps they've taken is to perform testing of future mailings. That's certainly one way to help avoid obvious problems in the mailing process. Covered entities should consider these and other quality-control and validation measures to help catch errors on the front end."

Aetna Case Offers Many Lessons for CEs

Of the mailing breach cases, the Aetna case is the most distinctive, and offers the most lessons for other covered entities and business associates into how to safeguard generally low-tech mailings, Pearce says.

"Obviously there was a breakdown at some point in the process here, and without knowing more about the facts it's impossible to say who should be held responsible for that breakdown," says Pearce.

Key to safeguarding PHI in mailings is to assure that comprehensive business associate agreements (BAAs) are in place and followed.

The basic elements a covered entity would want to include in a BAA with any outside contractor—including firms that handle mailings—are those that are required by the HIPAA Privacy regulation, Pearce says. For a business associate that handles mailings, he says, some of the key mandatory provisions would be those that:

1) establish the permitted and required uses and disclosures of PHI

2) obligate the BA not to use or disclose PHI other than as permitted or required, and

3) obligate the BA to use appropriate safeguards to prevent the use or disclosure of PHI other than as provided for in the parties' contract

Beyond those "basic foundational elements," Pearce says, the parties can specify particular handling requirements, either in the underlying services agreements or in the BAA.

He says the Aetna breach indicates that these requirements should include:

1) a duty to obtain the covered entity's prior written approval to the substance and form of the communication (this approval should probably come from the covered entity's privacy office), and

2) a requirement to limit the inclusion of PHI such as health condition and treatment information to the minimum necessary.

BAA is 'Just the Minimum'

The litigation surrounding Aetna's privacy breach provides "lessons and opportunities for all large health care organizations and health plans on steps or measures that they can use to better plan and produce written communications that are sent through the mail," says David Holtzman, vice president, compliance strategies, for CynergisTek, Inc.

If a vendor is used, "in order for the covered entity to disclose the PHI needed, there must be a business associate agreement in place that ensures the contractor or vendor will take appropriate measures to safeguard PHI," Holtzman says.

It's important to make a distinction between the business associate agreement and the contract covering the actual mailing, Holtzman says. "The business associate agreement is meant to only serve as minimum requirements for the contractor to stand in the shoes of the covered entity's obligation to safeguard PHI as required by the HIPAA rule," he says.

Covered entities will need two legal documents with a business associate responsible for a mailing, he says: the business associate agreement, and a contract covering the terms of the actual mailing.

"The point is that contract services and the business associate agreement each play an important and distinctly separate role in governing the relationship in successful production of mailings that are effective communication tools while protecting confidentiality," says Holtzman.

The litigation involving Aetna "discusses several mailings being made by various contractors for a number of different projects," he says. "In some cases, a contractor was hired to coordinate the development and production of materials that were mailed by subcontractors. In other instances, it would appear that mailings were being produced internally, without coordination or centralized management."

In Pearce's view, Aetna had policies in place requiring BA agreements but didn't follow them. This may leave it open to penalties from OCR, which are separate from the insurer's settlement in the class action lawsuit, he points out.

Consider 'Broad Management Approach'

The case shows that health plans need to put policies in place on mailings, Holtzman says. This policy should govern what information is being sent, the sensitivity of the data, and the exact medium used, "including whether it is appropriate to use a window envelope. Plans should consider whether the sensitivity of the member or patient information reasonably precludes the use of a window envelope."

For example, plans should consider whether to use a cover page to hide documents containing sensitive information, he says. And, "there should be an appropriate level of supervision in the design, production and quality assurance prior to sending."

In some cases, it may be better to produce the mailing in-house, while in others, a vendor may be the best choice, Holtzman says. But regardless, that decision "should be part of the planning stage—it's all part of the broader management approach, whether the production of the mailing piece is in-house or you intend to select a vendor."

If a vendor is used, the organization "should employ sound vendor management principles," he adds. "The RFP [request for proposal] should contain appropriate standards and requirements that would be needed to ensure that the mailing would be produced to meet the organization's standards and expectations. Organizations should also consider the minimum necessary amount of PHI that will be disclosed in order to produce the documents or envelope that will be sent."

Following vendor selection, the covered entity should "monitor the production of large-scale mailing projects to ensure that their contractor is meeting the requirements and expectations to safeguard the information. For example, if the vendor is receiving or creating PHI electronically or through an information system, the covered entity should ensure the business associate has conducted an information security risk analysis to identify threats and vulnerabilities, and [ensure] that risks to PHI have been reduced to a reasonable level," Holtzman says.

Covered entities also should require production samples prior to the actual mailing, "including quality assurance of the finished product at the last step prior to the delivery into the postal system," he recommends. In addition, if the contractor is using a subcontractor for all or part of the work, covered entities must ensure that their contractor will en-

force these same provisions for all subcontractors, Holtzman says.

Facility Type May Predict Breach Risk

What are the key lessons emerging from this case for covered entities?

According to Holtzman: "Put into place operating policies and procedures that apply to all business units in the organization to carefully plan and strategize the production and mailing of all documents that contain PHI to ensure that only the minimum necessary health information is used or disclosed, that the proper envelope or container is used to contain the document, and that good vendor management practices are used in selecting and contracting if outsourcing, including ensuring that a valid business associate agreement is in place."

Pearce adds: "One lesson covered entities and BAs can take away from this is to involve the privacy office in the vendor engagement and quality control process used for mailings. Those folks will be more attuned to the potential issues a mailing might pose, including those presented by a mailing vendor. Key quality control measures would include prior written approval by the privacy office for the substance and form of mailings and a requirement to limit the inclusion of PHI in any mailing to the minimum necessary."

See the CarePlus breach notice at http://bit.ly/2oKnR9b and the Tufts statement at http://bit.ly/2FSMCII.

Contact Pearce at alex.pearce@elliswinters.com and Holtzman at david.holtzman@cynergistek.com. ✧

Study: Low-Tech Breaches Involving Paper, Film Most Common in Hospitals

Paper records and films represent the most common types of data subject to breaches in hospitals, eclipsing electronic breaches such as ransomware, a study finds. These low-tech breaches are mostly due to theft, improper disposal and unauthorized access, according to the study, published in the *American Journal of Managed Care*, which also looks at the key factors leading to data breaches.

"As high-tech as the health care industry has become, there is still a large amount of paper usage, especially for facilities that were outside the scope of meaningful use," says study author Amanda Walden, Ph.D. candidate at the University of Central Florida, referring to standards for electronic medical records supported by federal funds. "As long as we have paper in use, there will always be manual processes that are susceptible to breaches, whether malicious—stolen records, or accidental—dialing the wrong fax number or losing a box of records."

The study examined at hospital-based data breaches reported to OCR between October 2009 and July 2016.

It identified 215 breaches affecting 500 or more individuals. Thirty hospitals had multiple breaches during that time: 24 hospitals had two breaches, five had three breaches and one had four breaches.

Data breaches involving paper or films occurred most frequently: the study identified 65 such breaches. Electronic data in "other locations" (e.g., laptops, desktops, email, electronic medical records, or network servers) were breached in 56 hospitals, and in laptops specifically, 51 hospitals, the study reports.

The likelihood of suffering a data breach depended in part on the type of facility, the study shows. Specifically, teaching hospitals, pediatric hospitals and larger hospitals were more likely to have a data breach, while investor-owned hospitals and specialty hospitals were less likely to have a breach.

However, regardless of the type of facility, the authors write, the overall number of patients affected by low-tech breaches was relatively small. Whereas breaches of network servers, though less frequent, can impact millions of patients overall.

Walden says the study indicates larger facilities have "a lot more ground to cover in terms of managing risk," and managing risk involves managing employees, especially when it comes to electronic breaches. Training is important, and should cover both paper and electronic breach examples, she says.

Because electronic breaches affect more patients, Walden says institutions' strongest focus should be on preventing high-tech breaches.

Walden tells *RPP* that she and her co-authors believe security is underfunded overall, and that, despite the study's findings about low-tech breaches, leadership in hospitals should focus on cyberbreaches. "Education on phishing/spearing for employees is critical," she says. "Also, the need for two-factor and biometric security technologies is important as well."

However, Rebecca Herold, president of SIMBUS360.com and CEO, The Privacy Professor, says hospitals need to cover both low-tech and high-tech breaches in their security training and awareness programs. Herold tells *RPP* that she's seeing the trend of non-digital breaches increasing, given that most organizations now focus on digital security. "Don't forget to protect all forms of information—you cannot

forget about low-tech decades-old types of security," she says.

Common Breaches Run the Gamut

The study's conclusion that low-tech breaches are more common rings true, says Herold. "Just think about the hospital environment—there are print copies of reports and patient images in an unlimited number of locations," she says. "And this is with patients and their visitors, along with the wide range of hospital workers, often with easy access to them." It also makes sense that digital devices are responsible for the largest breaches, she says, since they can store huge numbers of records in a format that's easy to steal or accidentally share.

Lowering the risk of breaches takes having a better understanding of the many ways they can happen. Common low-tech breaches include:

◆ Improper disposal of hard-copy media and images, along with digital media, which then can be taken by someone who sees the opportunity to get the protected health information (PHI). "We still see so many plans and providers getting breaches because they throw away hard copies into back alleys or dumpsters," she says.

◆ Donating old equipment to schools, charities, day cares and similar organizations without first removing the data from the devices.

◆ Selling old equipment that will no longer be used in an effort to recoup investment without first removing the data from the devices. "I've had situations where buyers, from used equipment stores or from eBay, actually call the hospital tech line to ask how to use the applications still located on the computers, and upon further investigation the hospitals found that all their patient files were still on the computers as well," Herold says.

◆ Discussing patients in public areas, such as in elevators containing visitors and patients. "This happens all the time," Herold says. "I just came back from a trip, and the people sitting behind me in the airport gate area waiting for their flight were discussing a patient and a very unique type of medical problem—and also said the patient's name. This is a HIPAA violation. If I could hear it, unauthorized access to that PHI occurred. Just imagine what I could have done with that information … or if I had been livestreaming that conversation online."

◆ Posting information about patients where others can see the information, such as charts on doors, facing outwards.

◆ Photos and videos that include in the images PHI, and also images of the patients themselves.

The culture of the hospital workplace also plays a role, Herold says—the top leadership of the organization needs to reinforce the importance of protecting privacy.

Read the full study at http://bit.ly/2EJmpel.

Contact Walden via *AJMC* spokesperson Theresa Burek at tburek@mjhassoc.com and Herold at rebeccaherold@rebeccaherold.com.✧

Blockchain: Network of the Future?

continued from p. 1

But Ngo suggests solutions can be gleaned from how the financial industry and its regulators have grappled with similar issues related to Bitcoin and other cryptocurrencies. Don't fret if confusion remains about blockchain because Ngo says there are newer hot concepts just around the corner.

RPP: Tell us about your interest in blockchain and how you got started with the concept.

Ngo: I have an MBA, which was information-technology focused. It kind of opened my mind to tinker around with many things. And through the years I've been able to build a relationship with quite a few very technologically-involved individuals, really high-level programmers, geeks, tech people. I was basically an early adopter of blockchain. In 2013, when Bitcoin was still early, I built machines to basically mine for digital currencies. And that's kind of the backbone of where my understanding of blockchain grew from. Bitcoin and blockchain are not the same thing. Bitcoin was the first implementation of a successful blockchain but [is] not Bitcoin. Blockchain is the underlying technology to it.

What exactly is blockchain? Is it a security technology or a network?

It's both. It's a heavily encrypted—it hasn't been hacked yet—distributed ledger that is verified by all parties that are plugged into the network. The easiest way to think about this is financially. If you want to transfer money to me and you're in the United States and I'm in, say, China, you have to send the money to the bank, to Bank of America [for example], and then Bank of America can do whatever it wants, takes its fees, logs it into its books, and sends the money over to me in China. So that's the traditional sense of logging data. Instead of having to transmit the money from you to Bank of America to me, with Bitcoin or blockchain, you can transmit the money directly to me, bypassing Bank of America. That's what Bitcoin did and that's what the blockchain allows.

What potential do you see for blockchain in health care and where do you think it might make the most sense?

It has phenomenal potential. I think it's going to be extremely disruptive. There are so many uses. Think of it in terms of ordering supplies, insurance billing and management. Let's take medical records. If you get sick in Argentina, you have to call the hospital system or wherever has your medical record. It's not distributed everywhere. With blockchain, the thinking is to have the data, or elements of the data, on the whole network where everyone has access to it. If I [as a treating physician] need to plug in and check your health record, you send me the authorization key from your phone. I can then plug into the network…and pull the data off the network without going through the medical records department of the hospital where you get all your care from.

Are there logistical issues that need to be worked out?

How we handle the large volume of data without allowing people to actually view the data unless they are authorized to [is one]. Because the more data you have on network, the slower the network gets, the more expensive it gets to transact data. To keep the data light and to keep the data secure, [perhaps] all you store on the blockchain for health care or health records could be a hash code that corresponds to that data. Then there are relatively centralized data centers, data nodes, set up around that store the real data. MRI scans, patient records, lab results, X-rays…the digitization of that data is very cumbersome.

Bitcoin is a public blockchain. Everyone can see who holds how much Bitcoin. So all the data is transparent, in that you see the address but you don't know who owns the address. When it comes to health care, it has to be a mix of a private and public blockchain where there's a hashtag that refers to data stored on a private blockchain or private network where no one can see the data.

I'm not a data scientist but I do know there are going to be attempts to [figure out] how you provide a public hash code or a public address that references data set up somewhere privately where it's completely anonymous or completely secured only until when it's released.

How much interest do you think there is right now among HIPAA privacy and security officers about this? Are they burying their heads in the sand and saying "Oh, Bitcoin isn't real and neither is blockchain?"

I think a lot of people are burying their heads in the sand, but I can tell you the venture capitalists are very interested and very involved. It's going to happen. I know health care is a little conservative but I think it's going to happen quicker than people think, especially if there are opportunities to capitalize on it. Entrepreneurs are going to jump in and figure out a way to make it work.

Where does the security rule under HIPAA fit in? It is often seen as an arcane framework.

I don't know. That's the government's problem to figure out. I would recommend that HIPAA [regulators] use the example of what's happening in the financial arena as a case study to figure out how they can proactively step up to regulate what's going to happen with the transmission of data for patients. Or they are going to be playing catch-up like the Securities and Exchange Commission [SEC] is doing.

What's happening now with initial coin offerings, ICOs, is that people are raising hundreds of millions, billions of dollars, without doing proper financial disclosures and the Securities and Exchange Commission is struggling with how to regulate it. Singapore…Great Britain…all these countries are having a problem trying to regulate the transmission of these funds and how these funds are being raised. The SEC's having problems regulating companies that are not incorporated in the U.S. but are, say, in Malta, in Gibraltar, in Switzerland, that are raising millions and millions of dollars.

What will it take for blockchain to take off?

There are two drivers in health care. One is the hospital systems jump on it, or [two] it's consumer-based and the patients jump on it. What's driving change in the financial sphere is the consumer who is the one that's saying, "Well, I'm not going to go through the banks anymore and let them track my funds and let the government have the ability to freeze my funds. I'm just going to hold my funds myself [in a digital wallet] and transact it myself," and that's what they're doing. There are companies that are starting to implement blockchain in health care. One is Patientory out of Atlanta (see https://patientory.com).

Medical billing is very expensive. The cost of medical billing to a physician's office is 6-10% [of revenues]. You automate that and you put it on the blockchain where there's already built in trust mechanisms through "smart contracts." You cut that cost down because you no longer need staff members to code and bill every chart and verify it on the other end with the insurance company.

Smart contracts?

That's a deeper discussion for another day! I want to point out though, that, I know we're using the term blockchain, but you should look into the technology called Tangoe. It's kind of a little bit different. In Tangoe, you have miners that verify the integrity of the data. [In addition], the Internet of Things Application—IOTA—is a technology that's being built right now that seems to be less cumbersome and potentially faster once it grows than a blockchain.

Contact Ngo at ango1@bidmc.harvard.edu. ✧

PRIVACY BRIEFS

◆ **The total number of health care records breached in 2017 hit a four-year low even as the number of hacking incidents increased**, according to the fourth annual Healthcare Breach Report from cloud access security broker Bitglass. This indicates health care organizations are doing a better job protecting data, the report concludes. The report, based on breach data from the U.S. Department of Health and Human Services, found that the number of breaches fell slightly—from 328 in 2016 to 294 in 2017. Excluding mega-breaches at Anthem, Inc., and Premera Blue Cross, the number of health care records breached dropped 72% between 2015 and 2017, the report found. "The number of hacking and IT incidents has increased, but organizations have done a better job mitigating damage, with 16,060 records compromised per breach on average in 2017," the company said. From 2014 to 2017, health care organizations reduced the number of breach incidents attributed to lost and stolen devices by 63%, the report found. Still, the cost per leaked record rose last year, from $369 in 2016 to $380 in 2017. Request a copy of the report at http://bit.ly/2I2W3FZ.

◆ **The Medical University of South Carolina (MUSC) fired 13 employees in 2017 after administrators** determined they had snooped in patient records without permission. Out of 58 privacy breaches at the institution in 2017, 11 were categorized as snooping, and some of those privacy breaches involved high-profile patients, MUSC said. Since 2013, MUCS says it has identified 307 breaches and has fired 30 employees as a result. Nearly half of all those firings occurred last year. None of those fired have been physicians, according to the institution. Read more at http://bit.ly/2sVIXaf.

◆ **A password-protected laptop stolen from a Houston city employee's vehicle may have contained medical records** containing names, addresses, dates of birth, Social Security numbers and other medical information of city employees. The laptop was stolen Feb. 2. The city had trained members of its human resources team not to remove laptops from city offices unless sensitive data was encrypted. "Because one employee failed to follow his training, all employees authorized to work with group health plan data are being re-trained to reinforce the prohibition against removing unencrypted data from the protections of city facilities," the city said in a statement. Learn more at http://bit.ly/2tbiXI2.

◆ **Western Washington Medical Group in Everett, Wash., says medical records and information for some of its patients may have been comingled** with regular trash in November, resulting in improper disposal. The medical group's janitor service mistakenly mixed documents in "shred" bins from the practice's orthopedic, sports, spine and hand group with other trash. The problem wasn't discovered until the next morning. The medical group says it believes that all of the disposed records were compacted in a trash compactor and are now part of a landfill; therefore, the medical group said, the risk to its patient population is low. The information contained in the "shred" bins may have included: names, addresses, diagnoses, medical history forms, appointment dates, medical history and health care insurance billing information. The janitorial employees have received additional training, the medical group says. View the statement at http://prn.to/2F7gfIV.

◆ **An internal medicine practice in Jemison, Ala., says it fell victim in December to a ransomware virus** that encrypted its electronic medical record software. Jemison Internal Medicine, PC, said it didn't pay the ransom demanded, "but instead removed the virus by reinstalling the operating system on its server and then restoring its patient records from backup copies." The practice's investigation found evidence that a hacker had gained access to its computer system, but no confirmation that the hacker had accessed any files within the electronic medical records system. Still, access was possible, so the practice notified 6,550 patients about the breach. Read the statement at http://bit.ly/2oFRYzs.

◆ **Personal details for 30,000 Medicaid recipients in Florida may have been accessed after a government employee fell victim to a phishing attack**, according to the state's Agency for Health Care Administration. The information obtained through the attack may have included full names, Medicaid identification numbers, birth dates, Social Security numbers and addresses, along with medical conditions. About 6% of victims had their Medicaid identification numbers or Social Security numbers potentially accessed, according to the agency. Read more at http://bit.ly/2GrarY2.

◆ **Hackers penetrated a business computer server at a dentist's office in Fresno, Calif.**, and may have copied or stolen data, according to the practice. White and Bright Family Dental said in a notification letter that the server contained patients' personal data, Social Security numbers, insurance information and dental history. View the notification letter at http://bit.ly/2FbNrLq.