Report on
Patient Privacy

Volume 19, Number 7 • July 2019

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

Claiming 'Certainty' of Re-Identification, HIPAA Violations, Patient Sues Google, U. of Chicago

A patient who was twice hospitalized at the University of Chicago Medical Center four years ago has filed a proposed class action suit against UC and Google, alleging UC gave his protected health information (PHI) to Google for use in a research study utilizing electronic health records (EHRs) without adequately de-identifying it. The suit terms UC's sharing of PHI with Google a "massive medical data grab."

UC and Google have called the suit baseless and said they would mount a defense.

The suit, filed June 26 in the U.S. District Court for the Northern District of Illinois, Eastern District, would have to be certified as class action litigation. It is being brought by Matt Dinerstein, who was admitted to UC medical center for a total of six days in June 2015. UC and Google began a research collaboration in May 2017.

UC, the suit claims, was "happy to turn over [to Google] the confidential, highly sensitive and HIPAA-protected records of every patient who walked through its doors between 2009 and 2016."

Both Google and UC "violated HIPAA by sharing and receiving medical records that included sufficient information for Google to re-identify the patients," the suit alleges. "Both were aware at the time of the transfer that the medical records contained information outside of HIPAA's safe harbor provisions, that a competent expert

continued on p. 9

Scrutinize Your Subcontractors Closely, Security Experts Warn Following Massive AMCA Breach

Covered entities (CEs) and business associates (BAs) need to re-examine their relationships with subcontractors and implement more stringent security protocols where necessary in the wake of the massive American Medical Collection Agency (AMCA) data breach revealed last month, security experts warn.

Details of the breach aren't completely clear—AMCA filed for Chapter 11 bankruptcy protection on June 17, and its bankruptcy petition includes a description of the breach. However, it is clear that health care industry consolidation, combined with outsourcing, means the size of potential breaches is increasing.

"Large data breaches will be more frequent, given the volume of IT outsourcing" and the amount of electronic protected health information (ePHI) held by health industry contractors, says Brian NeSmith, CEO and co-founder of Arctic Wolf Networks.

Roger Shindell, president and CEO of Carosh Compliance Solutions, adds that breaches aren't inevitable. "But a better job must be done in vetting of business associates," Shindell tells *RPP*. "The regulations actually require a covered entity to terminate their relationship with their business associate if the CE uncovers a pattern of non-compliance with the regulations and the non-compliance is not cured. This rarely happens, though."

continued

The AMCA breach, which may have involved more than 20 million patients, hit the clinical laboratory industry hard: Quest Diagnostics Inc. reported that it had nearly 12 million patients involved; competitor Laboratory Corporation of America Holdings (LabCorp) had 7.7 million patients involved; and BioReference Laboratories Inc., a subsidiary of OPKO Health, had nearly 425,000 patients involved.

The breach went undetected for more than eight months—from last August until late March—and then wasn't immediately reported. The affected companies first alerted stockholders in filings with the Securities and Exchange Commission.

In its bankruptcy filing, AMCA stated that it first became aware of a potential problem when it received a series of common point of purchase (CPP) notices. When credit card fraud is detected, banks analyze the data to identify the "point of purchase" the cards have in common, since that business could be the source of the data breach generating those stolen credit card numbers.

In response to the CPP notices, AMCA reports in its bankruptcy filing that it "shut down its web portal to prevent any further compromises of customer data, and engaged outside consultants who were able to confirm that, in fact, [AMCA]'s servers (but not [AMCA]'s mainframe) had been hacked as early as August 2018." This hack led directly to the bankruptcy filing, the petition said, as LabCorp, Quest, Conduent Inc., and CareCentrix Inc., the company's four biggest clients, either terminated or substantially curtailed their business relationships with AMCA.

AMCA said in its petition that IT consultants cost it $400,000 to determine the source of the breach. In addition, breach notification cost it "in excess of $3.8 million," which "required more liquidity than [AMCA] had available."

The company faces additional legal trouble. Two state attorneys general—Connecticut Attorney General William Tong and Illinois Attorney General Kwame Raoul—have opened formal investigations into the breach, and a third—Michigan Attorney General Dana Nessel—has asked for additional information from the company.

Also, multiple class action lawsuits have been filed against AMCA and its clients, including LabCorp and Quest Diagnostics. The class action lawsuits claim that the company delayed notifying victims of the data breach, and failed to implement security that could have prevented the breach.

Do Companies Properly Vet Contractors?

It's not clear exactly what might have caused the breach. AMCA has not provided details publicly beyond what it wrote in its bankruptcy filing. But HIPAA security experts say there are specific steps CEs and BAs should take in the wake of this breach.

Shindell acknowledges that he's speculating on the cause of the AMCA breach, but he notes that "in my experience, credit card processing firms tend to rely on PCI [payment card industry] as their go-to security protocol. Adding a HIPAA-focused privacy and security program would be beneficial."

Generally speaking, Shindell says, "most organizations do an inadequate job of evaluating their business associates for their HIPAA compliance. Spending more time in this kind of evaluation would have a significant impact in mitigating the possibility of a breach occurring."

David Harlow, principal at the health care law and consulting firm The Harlow Group LLC, also declines to speculate on what the companies involved could have done to prevent this particular breach. But he did offer some general guidance.

"I believe that a certain percentage of breaches are in fact inevitable, because not [all] vulnerabilities known to black hat hackers are known to white hat hackers or security professionals in advance of exploits, and not all known vulnerabilities are patched," Harlow tells *RPP*.

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.

Subscriptions to *RPP* include free electronic delivery in addition to the print copy, as well as a searchable database of *RPP* content and archives of past issues at compliancecosmos.org.

To order an annual subscription to **Report on Patient Privacy** ($485 for HCCA members; $565 for nonmembers), call 888.580.8373 (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.

"However, many significant breaches over the years have been due to poor data hygiene, including the failure to prioritize sufficiently the preventive measures necessary to frustrate bad actors." These include patching systems as soon as they are made available, and auditing the compliance capabilities and practices of BAs, he says.

Harlow adds, "Implementing best practices consistently may not necessarily have avoided this latest breach, but doing so would have prevented many of the breaches we've seen in the headlines."

Specific Steps Urged to Manage Vendors

Obviously, a CE that uses BAs is dependent on those BAs to safeguard protected health information. But that doesn't mean there's no role for the CE to play, NeSmith says.

"This is a matter of vendor risk management and ensuring that the people you are doing business with have adequate security controls to protect your sensitive data," says NeSmith. "If someone has outsourced IT services, it is incumbent on them to ensure that they have decent security in place. While there is no way to absolutely guarantee security in someone else's environment, vetting and auditing your vendors can minimize the risk."

Shindell adds that CEs and BAs should ask their subcontractors very specific questions, which should include: "Did the BA conduct a risk assessment" as per the National Institute of Standards and Technology (NIST) *Guide for Conducting Risk Assessments*—NIST SP 800-30 Rev. 1 (2012)? "Did they generate a remediation plan? Is there a policy and procedure manual developed through the remediation process? Do they conduct adequate training? Can they provide documentation attesting to the above?"

NeSmith points out that businesses have different appetites for risk, which will affect security protocols and how they choose their vendors. "Covered entities and business associates need to arrive at their risk appetite and make the investments to meet that goal. Covered entities need to ensure they are properly vetting their business associate supply chain and auditing that supply chain." NeSmith adds that he has seen some CEs and BAs using the Standardized Information Gathering (SIG) and SIG Lite questionnaires to qualify their subcontractors.

BAs and subcontractors need to undergo "comprehensive review" before they are entrusted with data, Harlow says. "This includes requiring them to complete comprehensive questionnaires and assessments." Regular audits also are essential, he says, adding, "this is not a 'set it and forget it' kind of function."

Look for vendors who have taken steps to earn certification, Harlow recommends. "The best indication of vendor preparedness to deal with known and unknown security vulnerabilities and breaches [is] internal or third-party attestation of compliance with broadly

continued on p. 4

PATIENT PRIVACY COURT CASE

This monthly column is written by Homaira Hosseini 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 Homaira at homaira.hosseini@morganlewis.com.*

◆ **Class action lawsuit filed against Ancestry.com for breaching HIPAA and sharing private health information**. In April 2019, Alameda County Superior Court accepted a class action lawsuit against Ancestry.com (Ancestry). The class action suit alleged that Ancestry released clients' private health information without express permission or written authorization. The state court class action complaint alleges that Ancestry's notice of disclosure is insufficient to allow Ancestry to release the private information of its patients under applicable law.

On June 27, 2019, Ancestry removed to California federal court. The notice of removal described the class of Ancestry customers "who purchased DNA products from Defendants in the State of California" and whose "personal information" was purportedly "compromised after purchasing genealogical services from [Ancestry]." The class exceeds 100 members, and the amount in controversy exceeds the sum or value of $5 million. The class alleges that pursuant to federal and California law, Ancestry is a health care provider and is required to keep medical information private. The class argues that Ancestry willfully breached their fiduciary duty of confidentiality, pursuant to the HIPAA Privacy Rule 45 C.F.R. § 160.103 (2018) and 45 C.F.R. § 164.530 (2018), by failing to protect the personal and DNA data. (*Collett v. Ancestry.com DNA LLC et al*, No. 4:19-cv-03743 (N.D. Cal. filed Jun 27, 2019)).

continued from p. 3

accepted standards—e.g., NIST Cybersecurity Framework or HITRUST CSF."

Automated processes that limit key human factor vulnerabilities also are important, he says, noting that "reducing in a responsible manner the number of human touches required for all functions of the BA or subcontractor will likely increase the security of the data in question."

NeSmith points out that companies should actively monitor systems and have a plan they can implement instantly if a breach occurs. "Contractors need to have adequate security that includes protective measures and detection so you can slam shut the window of vulnerability once something gets compromised," he says. "Having adequate monitoring can mean the difference between a compromise and a catastrophic data breach."

Regular review of data minimization and data segmentation practices also is critical, Harlow says. "Does your BA need to have all of the data? Could it be segmented or anonymized or de-identified in a manner that still allows the BA to discharge its functions? Some level of inconvenience and expense is worthwhile if it can help minimize the chance of a significant data breach."

Finally, it's important to perform real-world tests, such as those involving fake phishing emails, to see where security is lax or could be improved, Harlow says. "If they click where they shouldn't, they get re-education rather than triggering a breach." Humans often are the weakest link in the entire security infrastructure, he points out. Real-world tests should include simulated cyberattacks in the form of penetration testing, he says, as "these are a critical component of any robust data security system."

Security requires CEs and BAs to take multiple steps in a variety of systems, experts say. "Most breaches are not terribly high-tech," Shindell says. "Most breaches are caused by a series of small mistakes that grow. Training is the cornerstone of a robust security and privacy program. OCR suggests that almost all breaches can be tracked back to inadequate training being a contributing factor."

The AMCA data breach shows that CEs and BAs need to "up their game" to protect ePHI, which includes monitoring their environment to detect threats that might slip through, NeSmith adds. "Covered entities will probably be imposing more rigorous vetting and auditing for their IT outsourcing relationships. Business associates can expect to spend more time and resources demonstrating to their partners that they are following cybersecurity best practices."

Contact Shindell at rshindell@carosh.com, Harlow at david@harlowgroup.net or via his blog HealthBlawg, and NeSmith via spokesperson Melanie Ford at ford@merrittgrp.com. ✧

Checklist for Subcontractor Management

In the wake of the American Medical Collection Agency breach, which affected at least 20 million people, HIPAA security experts recommend the following steps for covered entities and business associates to take in order to safeguard any of their own electronic protected health information that might be in the hands of a subcontractor:

- Consider your overall risk tolerance and invest in security accordingly.
- Scrutinize your supply chain partners before you contract with them.
- Look for partners that comply with accepted standards, such as the National Institute of Standards and Technology Cybersecurity Framework or HITRUST CSF.
- Audit your supply chain partners regularly to make certain their security protocols remain up to date and tight, and that they are complying with HIPAA regulations.
- Regularly review whether your BAs have access to too much electronic protected health information, and reduce access where necessary.
- Install and test patches as soon as they become available.
- Conduct real-world and job-function-specific data security training and testing.
- Conduct regular audits of your entire security infrastructure, including penetration testing.
- Make sure you can immediately shut down access to systems if something does get compromised.
- Expect to spend more time and resources overall on security.

On Heels of OCR's Reduction In Fines, Congress Offers Its Views

In the roughly three months since the HHS Office for Civil Rights announced it planned to reduce the amount of fines imposed for all but the most serious HIPAA violations, OCR issued two settlements—but both were finalized before the change.

The health care privacy and security community, then, has yet to see how the recent decision by OCR Director Roger Severino plays out and, at the same time, what impact there might be on compliance.

Now Congress has entered the fray. Significant health care legislation is advancing in the Senate that calls for OCR, when dealing with HIPAA violators, to take into consideration whether a covered entity (CE) or business associate (BA) had "recognized security practices in place" for at least a year that would "mitigate fines" or "limit remedies" the agency might impose.

It could be argued that OCR already does this, but in recent years, particularly as its penalties have risen, the agency has stopped explaining how it arrived at settlement amounts. For example, last year OCR entered into a $16 million settlement with Anthem Inc. over a massive exposure of protected health information (PHI)—some 79 million records were involved. Severino said only that the "largest health data breach in U.S. history fully merits the largest HIPAA settlement in history" ("OCR Exacts Its Pound of Flesh From Anthem With $16 Million Settlement, Corrective Actions," *RPP* 18, no. 11).

Now Annual Caps Will Vary

Although specific decisions in individual settlements are not always disclosed, OCR's penalty structure since it implemented the 2009 HITECH Act has been based on four tiers with amounts assessed per violation and per year, with an annual cap for identical violations.

The tiers range from $100 per violation minimum for acts that an organization (defined as a person under the law) did not know "and by exercising reasonable diligence," would not have known, that the person violated a HIPAA provision to $500,000 for willful neglect and when the violation has not been corrected within 30 days.

Despite the differences, OCR has been applying a maximum of $1.5 million per year for all of the tiers, rather than at just the top or highest level of culpability.

It may be appropriate to thank the University of Texas MD Anderson Cancer Center for the reduction, as it came in the middle of a legal battle it is waging against a multimillion-dollar fine OCR has been trying to impose since 2017.

MD Anderson refused to settle and took its concerns to an HHS administrative law judge; in July 2018, OCR announced that the ALJ upheld the agency's intent to impose a fine of $4.358 million on MD Anderson for a stolen laptop and a USB drive lost in 2012 and $1.5 million for another drive reported missing in 2013. To this total OCR added $1.348 million for failing to implement access controls, specifically encryption and decryption ("Lack of Encryption Key to $4.3M Penalty For MD Anderson; 'Layered Security' One Solution," *RPP* 18, no. 7).

Penalty Drop Followed MD Anderson Litigation

In April of this year, MD Anderson filed suit against HHS Secretary Alex Azar in the U.S. District Court for the Southern District of Texas; it is arguing, among other things, that OCR lacks the authority under HIPAA to fine MD Anderson because it is a type of state agency and that the fines imposed are excessive ("Should 'State' Agencies Be Exempt From HIPAA? MD Anderson Says Yes," *RPP* 19, no. 5).

MD Anderson also specifically called out the fact that OCR's calculations of its penalty equated to "the maximum amount that the OCR could impose under any level of culpability under HIPAA, making the punishment the same as in a case in which [electronic protected health information] was intentionally taken to cause harm to patients and where harm was actually incurred." The cancer center said the fines were in violation of annual caps imposed per identical violation.

That will change with settlements OCR reaches now. As Severino announced on April 26, OCR has changed its interpretation of the law and instead intended, from that day forward, to impose annual maximums of $25,000, $100,000 or $250,000 per year for the three lower tiers of violations.

As of *RPP*'s deadline, HHS had not yet filed a formal response to the suit. But the reduction in the annual caps clearly seems to be connected. MD Anderson officials told *RPP* the "revised penalty structure interpretation is consistent with MD Anderson's legal arguments" and that they were "hopeful the OCR will reexamine the proposed penalty against MD Anderson consistent with its new approach."

In announcing the reduction, OCR did not tie its decision to anything other than a "more accurate" reading of the HITECH Act, and HHS has stuck to its position of not commenting on pending litigation ("Easy Win for MD Anderson? OCR Drops Annual Caps, Issues Warning on Right-of-Access Denials," *RPP* 19, no. 5).

As noted, OCR has issued two new settlements since that April announcement, but they were completed before a reduction could go into effect. The seeming disparity in the amounts and size of the breaches at the center of the settlements could perhaps be seen as an argument for more standardization of penalties. At least one HIPAA expert advises against a focus on financial penalties (see following story).

Touchstone Medical Imaging LLC, OCR said on May 6, agreed to a $3 million settlement for a breach affecting 307,000 individuals ("$3 Million Settlement Demonstrates Need for Quick Breach Management," *RPP* 19, no. 6). The circumstances included a delay in notification of the 2014 breach that occurred when a patient billing file was "inadvertently" available online.

Then, on May 23, the agency announced a $100,000 agreement for a breach that affected 3.9 million medical records held by Medical Informatics Engineering, a business associate (BA) ("Generic 'Tester' Accounts Allowed Records Hack Triggering $1M in OCR, State AG Payments," *RPP* 19, no. 6). This firm, however, paid another $900,000 to settle a suit brought by 16 states.

Compliance With NIST Standards Favored

Proposed changes to the HITECH Act are found in the Lower Health Care Costs Act, S. 1895, 116th Cong. (2019). The bill was introduced on June 19 by Sen. Lamar Alexander, R-Tenn., chairman of the Health, Education, Labor and Pensions Committee, which Alexander chairs. The committee passed the bill by a 20-3 vote on June 26; it now will be considered for a vote by the full Senate. The bill proposes a series of reforms, including management and oversight of "surprise" bills and drug costs.

Provisions affecting HIPAA penalties are part of a section on improving the exchange of health information.

The bill would amend the HITECH Act with a new section titled "Recognition of security practices." It specifically references guidance issued by the National Institute of Standards and Technology, as well as "any other program or processes that are equivalent to such requirements as may be developed through regulations." S. 1895 would allow CEs and BAs to identify the practices.

Addressing OCR (technically HHS), the bill states that "when making determinations relating to fines," when "decreasing the length and extent of an audit" or when contemplating "remedies otherwise agreed to by" HHS, the agency "shall consider whether the entity or business associate had, for not less than the previous 12 months, recognized security practices in place that may…mitigate fines," take action that would "result in the early, favorable termination of an audit" and "limit the remedies that would otherwise be agreed to in any agreement" between HHS and a CE or BA.

It also provides that the CE or BA, if it chooses, can ask HHS for "further consideration by adequately demonstrat[ing] that such recognized security practices were in place."

The bill also calls for the Government Accountability Office (GAO) to conduct a study that could end up making the case for an expansion of HIPAA to encompass firms that don't today have to comply, or it may prompt new regulatory efforts. The study appears designed to pinpoint risks and gaps in safeguards for electronically exchanged information.

GAO to Review Private Sector Protections

Were the bill to be signed into law, GAO would have one year from then to complete the study. GAO is being asked to "describe the roles of federal agencies and the private sector with respect to protecting the privacy and security of individually identifiable health information transmitted electronically to and from entities not covered" by HIPAA.

GAO also would "identify recent developments regarding the use of application programming interfaces to access individually identifiable health information, and implications for the privacy and security of such information."

The committee then wants GAO to review how the information that a person directs to be sent to or from a noncovered entity or BA is protected. GAO is to "identify practices in the private sector, such as terms and conditions for use, relating to the privacy, disclosure, and secondary uses of individually identifiable health information transmitted electronically to or from entities, selected by an individual" that are not covered by HIPAA.

More broadly, the committee has asked GAO to "identify steps the public and private sectors can take to improve the private and secure access to and availability of individually identifiable health information." ✧

Deterrent Effect of OCR Fines Unknown; Expert Advises Against 'Rolling the Dice'

Little is known about the possible deterrent effect of fines levied by the HHS Office for Civil Rights (OCR) for HIPAA violations on compliance; no studies appear to have been published on the topic. OCR's settlements can lag the actual breach of violation by up to five years, perhaps diluting a potential impact.

Many of the newly announced settlements surround old problems, like lost or stolen unencrypted laptops and mobile devices, or a near-universal failure

to conduct a security risk analysis—or one that meets OCR's definition of "comprehensive."

Certainly there has been an increasing number of large-scale breaches at the same time that OCR's fines have reached a record high.

Nevertheless, compliance officials use OCR's big fines to incentivize (or, essentially, scare) workers into following hospital and other privacy and security policies, a situation that may lead to a clampdown of legitimate information sharing, particularly with patients and families.

In recent years, OCR has sought to fight this urge, particularly when it comes to combating the opioid crisis. In 2017, OCR issued "clarifying guidance" specifying four specific situations in which providers can share information, particularly following an opioid-related hospitalization, with family members or friends without expressed authorization ("OCR: After an Opioid Overdose, Sharing Patient Information Can 'Help Save Lives,'" *RPP* 17, no. 11).

Penalty Focus May Be Counterproductive

Further, in April OCR announced that it was dropping the annual cap for all but the most serious violations, a move that potentially could result in far fewer million-dollar settlements, and the Senate is also addressing penalties (see story, p. 1).

But at least one expert tells *RPP* focusing on the possible financial consequences of getting caught violating HIPAA is a bad move anyway.

"I'm not really telling people about the drop in fines," says Jeff Drummond, a partner with Jackson Walker LLP in Dallas.

"Even with the drop," he points out, "the fines will still be potentially crippling to a small business." In addition, organizations "should be compliant anyway because it's better for their business even if they only get a small fine."

He notes it's important to remember OCR isn't the only enforcer on the block.

"Even if there were no HIPAA fines, there's still the possibility of state law actions," says Drummond. This fact has been in evidence over the years on occasion, but recently reached a new level.

In May, Medical Informatics Engineering settled a suit with 16 state attorneys general for $900,000 for a 2015 breach, demonstrating a new level of cooperation among state officials ("Generic 'Tester' Accounts Allowed Records Hack Triggering $1M in OCR, State AG Payments," *RPP* 19, no. 6).

There is also the virtual certainty that any organization suffering a prominent breach will face a class action suit, which may be more costly to resolve than either federal or state enforcement actions, Drummond notes. Anthem is just one example. Before settling with OCR, Anthem paid $115 million to end a class action suit ("$115M Settlement Ties Anthem to Security Upgrades, Certain Staffing, Spending Levels," *RPP* 18, no. 9).

Drummond also urges common sense: "It's really bad for a health care business' reputation to be considered to be lax with patients' privacy. Anyone who thinks [lower fines from OCR] is a 'get out of jail free' card is missing the point entirely."

He counts himself among the group who "for a long time…have argued that an enforcement regime that meted out more fines and punishments would be more effective at focusing the industry on HIPAA compliance."

Fines of $1 million or so "isn't reasonable and would drive a lot of folks out of business," says Drummond, adding "it appears that OCR had settled on an enforcement strategy of big, headline-producing fines, but only against big players who should be doing a better job at HIPAA compliance since they have bigger budgets, not to mention bigger pools of protected health information, and need to get hit with a two-by-four to get their attention."

He observes that "you could fine a big hospital system $10,000 every day and it might not be a big enough burden to force real changes in behavior."

Would 'Speed Bumps' Be More Effective?

As a result of OCR's approach to date, the environment has been created where covered entities, says Drummond, "know that if they get fined it will be huge—and possibly kill the business—but that the likelihood of a fine is very small."

In Drummond's view, this can breed complacency and an attitude of "let's roll the dice and hope for the best."

Leaders may think "we have to spend a lot on enforcement and might still get a kill-the-company fine if something goes wrong," but given the rarity of settlements, "it's extremely unlikely that we will ever get in trouble," says Drummond.

Instead, what could be more effective is what Drummond calls a "speed-trap strategy."

OCR could conduct "many" and perhaps "more cursory" investigations and impose more fines, "but with the dollar amounts set to be painful but not deadly," says Drummond. This could work like a known speed trap where "everyone is more likely to drive slowly," or, in this case, abide by HIPAA.

Contact Drummond at jdrummond@jw.com. ✧

Judge in Ciox Health Case Tells HHS 'Let Me Rule'; Sets New Deadlines

Barring any delays, by the end of this month a district court judge should be able to consider how to rule on whether the nation's largest medical records retrieval firm can at least challenge the fees set by the HHS Office for Civil Rights (OCR) that apply when individuals seek protected health information (PHI) from providers.

On June 28, Ciox Health LLC met the deadline set by Judge Amit P. Mehta with the First District Court for the District of Columbia for it to "supplement the factual record to support its theory of standing" and/or submit a "memorandum of no more than ten double-spaced pages that explains how any new evidence affects the standing calculus."

The case is being watched by patient advocates and other medical records firms, especially those like ChartSquad LLC that fulfill requests on behalf of patients and have themselves been urging OCR to take action against fee violators ("Suit Raises Hopes OCR's 'Hot Mess' of Access Enforcement Will Be Fixed,'" *RPP* 18, no. 2).

Ciox, a business associate (BA) under HIPAA, filed suit in January 2018 ("Medical Records Firm Sues HHS Over Access Fees, Seeks Return to System Under State Laws," *RPP* 18, no. 2). In sum, the firm contends OCR's allowable fees are "irrational, arbitrary, capricious, and absurd" and questions the applicability of a fee of $6.50 per request as applied regardless of where the records are headed. Ciox argues it should be allowed to charge more for third-party requests and that OCR is violating the spirit and the letter of the HITECH Act. Ciox said it is following OCR's 2016 guidance on fees, which it refers to as "mandates."

OCR issued a series of three guidance documents on the topic ("For the Third Time, OCR Weighs In on Allowable Fees for Patient Records," *RPP* 16, no. 6). For all the guidance documents, visit http://bit.ly/2C0IL8J.

The impetus for the litigation was OCR's attempts to take enforcement action against Ciox under the belief it was violating the fee schedule. In responding to the suit, however, HHS claimed it lacked authority to pursue BAs for fees, only covered entities (CEs). To back up this position, OCR on May 24 issued a surprise "fact sheet" on BA liability without mentioning the suit. *RPP* discovered, however, that HHS attorneys also filed it in the district court as part of their response to the suit ("New OCR Fact Sheet on Business Associates' Liability Part of Move to Dismiss Suit Against HHS," *RPP* 19, no. 6).

Judge Sides With HHS on Fact Sheet

Ciox's attorneys were dismissive of the fact sheet; Mehta was not. "Knowing it cannot win on the substance, HHS has employed every trick short of renting a billboard outside the courthouse to convince the court that Ciox lacks standing and that the court may not resolve the merits in Ciox's favor," the firm responded on May 30. Ciox called the fact sheet "the latest in a series of post hoc policy reinventions."

But on June 4, Mehta ruled that the fact sheet supports HHS's claim that it lacks jurisdiction to take action against Ciox, and thus Ciox lacks standing to bring the case on grounds that it's facing enforcement action. However, he is allowing the case to move forward on the grounds that Ciox may have suffered harm based on the agency's fee schedule and established a series of deadlines to move the case forward.

The first deadline was June 28 for Ciox to file more arguments for standing, in the wake of the fact sheet, which Mehta termed "yet another attempt to clarify waters already muddied by ambiguously drafted regulations and the agency's shifting positions about their meaning."

He also expressed exasperation with HHS, writing, "At some point, the agency must stop clarifying and allow this court to rule."

In its June 28 filing, Ciox pushed back against Mehta's position that HHS has really let it—and other BAs—off the hook by virtue of the fact sheet.

"We respectfully disagree that HHS's posting of a 'Fact Sheet' on its website undermines Ciox's 'direct' standing,'" the new documents state. "Until this litigation was filed, HHS never once suggested that it lacked authority to enforce the challenged fee regulations against business associates."

'That Can't Be Right'

The medical records firm pointed out that OCR could remove the fact sheet "tomorrow and initiate enforcement action against Ciox for violating any of the rules Ciox challenges in this case. Indulging HHS's gambit effectively would allow the government to moot any case simply by posting a statement on its website that disclaims intent to enforce the law, creating an endless cycle that would derail the resolution of virtually any challenge to any administrative action."

According to Ciox, "That can't be right, and it isn't."

Ciox explained that its business model is to charge the hospitals it works for nothing to fulfill record requests submitted by patients and, instead, impose fees on attorneys and other third parties. As a result of OCR's 2016 guidance, Ciox "no longer is allowed to charge the rates it previously could and so has lost money."

It referred to HHS's position as a "mantra-like invocation of its [belief] that Ciox's [financial] injuries result from contracts it voluntarily made with its covered

entities, and that Ciox's supposed lack of foresight in structuring its business around nearly two decades of uninterrupted HHS policy is what's really producing Ciox's losses."

HHS, Ciox argues, "repeatedly claims that Ciox can avoid this allegedly 'self-inflicted' injury by renegotiating its contracts to permit Ciox to remain in business, or, taking HHS's position to its logical conclusion, that Ciox could simply leave the ROI [release of information] business if it doesn't like the new rules."

As it had in the initial complaint, Ciox argued that OCR's 2016 "mandates" on fees is not law, nor is the new fact sheet, and it chided OCR for not following a normal rule-making process that involves notice and comment.

According to Mehta's order, HHS now has until July 12 to respond to Ciox's latest filing. Mehta also gave Ciox until July 19 to rebut whatever HHS files, after which time he is expected to rule on standing. Should he agree that Ciox has standing, the case will move forward. It will then be months before any ruling on the merits of the case itself will be known.

In the alternate, a decision against standing could come sooner but likely would be appealed. ✧

Suit: U. Chicago, Google Violated HIPAA

continued from page 1

determination was not made, and that the thousands of patients had not given proper consent to allow Google to take possession of the records for the purpose of creating a commercial product."

Little information is available about how data were scrubbed of PHI. Just one paper appears to have resulted from the UC-Google project so far. Titled "Scalable and accurate deep learning with electronic health records," the paper was published last year in the Nature Partner Journals: *Digital Medicine*.

Using "de-identified EHR data from two U.S. academic medical centers with 216,221 adult patients hospitalized for at least 24 hours," authors from UC, Google, Stanford Medicine and the University of California San Francisco (UCSF) wrote that they "demonstrate[d] that deep learning methods using this representation are capable of accurately predicting multiple medical events from multiple centers without site-specific data harmonization."

According to the paper, "All electronic health records were de-identified, except that dates of service were maintained in the UCM [University of Chicago Medicine] dataset. Both datasets contained patient demographics, provider orders, diagnoses, procedures, medications, laboratory values, vital signs, and flowsheet data, which represents all other structured data elements (e.g., nursing flowsheets), from all inpatient and outpatient encounters. The UCM dataset additionally contained de-identified, free-text medical notes. Each dataset was kept in an encrypted, access-controlled, and audited sandbox. Ethics review and institutional review boards approved the study with waiver of informed consent or exemption at each institution."

A few more details are contained in a May 2018 article about the collaboration with Google posted on UC's website. Its Center for Research Informatics (CRI) "has a team of data warehouse staff dedicated to providing de-identified data for research," the post states. "The team has built a reputation for providing high-quality data for research while going to great lengths to protect patient privacy and security."

The post adds that "all patient identifiers, such as names, dates of birth, Social Security numbers and any other unique characteristic or code, were stripped from the data before Google was given access." The research, UC said, "was conducted according to our rigorous standards" and was "supervised" by the institutional review board (IRB) of UC's Biological Sciences Division.

Few Details Support Allegations

The group of attorneys representing Dinerstein did not respond to *RPP's* questions about the suit. Dinerstein, the suit claims, "never gave his written consent—or any consent whatsoever—to the university to disclose his confidential medical information to Google. Similarly, he did not give…Google permission to use his medical records for any purpose, let alone for a commercial purpose."

No patient authorization is required for research that uses de-identified data, but de-identification must follow HIPAA requirements.

No information about data use or other agreements between UC and Google is included in the suit (or in the published paper). Such agreements can (and in some situations must) prohibit re-identification by the recipient of the data. In addition, whether Google actually re-identified the data is not addressed in the suit.

Dinerstein claims that calling the data de-identified in the project is "incredibly misleading," because of the possibility of re-identification, which Google is "uniquely" positioned and qualified to perform.

According to the suit, Google's "geolocation information, when combined with the exact date stamps for admission and discharge (along with other health events at the hospital) included in the university's medical records, and cross referencing the age, gender, and demographic information with its own data, creates a

perfect formulation of data points for Google to identify who the patients in those records really are."

In addition, the EHR data included free-text notes that are not "normally" part of de-identified records and "create an enormous wealth of data re-identifying the patients themselves," according to the suit.

Without providing details, the suit contends that "the process used to redact the free-text notes, and its specific results, were not properly audited or verified in an independent manner. As such, there is no available information regarding the rate of personally identifying information that may have evaded redaction and was transferred to Google."

As such, "it remains a complete mystery to the patients whose records are now in the hands of Google," the suit alleges, as to whether the "methods and design of this software…could comprehensively review and redact millions of data points."

Injunction Sought Against Google Payments

Without citing any evidence, the suit claims that "Google's overtures for such detailed and identifiable records from hospitals, researchers, and healthcare providers alike were all uniformly rebuffed…until Google came across" UC.

Further, the suit states that UC "should not be permitted to retain any money derived from its provision of medical records to Google because it did not have authorization to give those records to Google." It does not provide any details on how much, if anything, UC has been paid.

The privacy rule provides a research exception to the prohibition and limits on the sale of PHI.

HIPAA does not allow a HIPAA covered entity to "sell" protected health information for purposes of marketing, except with patient authorization.

When it comes to the sale or receipt of remuneration when data is exchanged for research purposes, no authorization is required. However, Google (or other research partners) would be allowed to pay UC a "reasonable cost-based fee to cover the cost to prepare and transmit" the PHI for the research purpose.

The suit seeks an injunction requiring UC "to comply with all HIPAA de-identification regulations and enjoining [UC] from disclosing identifiable patient medical records to third parties without first obtaining consent," similarly an injunction "prohibiting Google from using patient records obtained from" UC, and an order "requiring Google to delete all patient records received" from UC.

The suit alleges that UC "provided Google a partner willing to turn over the information that it desperately needed" and that UC was "seeking not much more than notoriety for its collaboration with Google in the development of healthcare products." It offers no information about why Dinerstein believes his data are among that provided to Google or what type of misuse, if any, occurred. Stanford and UCSF were not named in the suit.

"Google tracks consumer locations through a variety of means including users of Android phones and its mobile applications, like Maps and Waze," the suit says. "Likewise, when a consumer uses other Google products, such as its search engine, Google records his or her Internet Protocol address, which corresponds to a very specific physical location. Google is, therefore, able to identify hundreds of millions of individuals' exact location within a matter of feet, if not inches, twenty-four hours a day."

Date Stamps Could Lead to Re-Identification

"Beyond the vast amount of personal information Google possesses, and its incredibly powerful analytics capabilities (including DeepMind Health), Google has in its possession detailed geolocation information that it can use to pinpoint and match exactly when certain people entered and exited the University's hospital," the litigation continues. "Based on these detailed profiles alone, Google has access to public and nonpublic information that could easily lead to the re-identification of the medical records it received. However, when the transfer of medical records is made to Google, the ability to re-identify those records becomes a certainty."

According to the suit, Google and UC publically "touted the security measures used to transfer and store these records, along with the fact that they had been 'de-identified.' In reality, these records were not sufficiently anonymized and put the patients' privacy at grave risk. The inclusion of, at the very least, the date stamp data immediately places the transfer of this medical data outside of the safe harbor provisions of HIPAA" related to de-identification.

Without providing evidence, the suit states that despite being "required by HIPAA, the university did not perform an expert determination before transferring the medical records to Google; or, alternatively, if it did make that attempt, any finding that 'the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information' was woefully misplaced."

Also without providing any details, the suit claims that UC "engaged in a cover-up to keep the breach out of the public eye so as to avoid the public backlash."

Dinerstein and other potential members of the proposed class action suit "suffered damages in the amount of the difference between the price they paid for the university's services as promised and the actual diminished value of its health care services," the suit alleges. "In addition, the individuals have suffered and will continue to suffer other forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses." No details were provided.

UC, Google: Rules Were Followed

UC Chicago would not respond to specific questions from *RPP* about the suit; it provided the following statement.

"The claims in this lawsuit are without merit. The University of Chicago medical center has complied with the laws and regulations applicable to patient privacy. The medical center is committed to providing excellent patient care and to protecting patient privacy."

"As a leading research institution, the medical center also pursues research partnerships to advance health care, improve patient outcomes and find cures for diseases. The medical center entered into a research partnership with Google as part of the medical center's continuing efforts to improve the lives of its patients," UC's statement continues. "That research partnership was appropriate and legal and the claims asserted in this case are baseless and a disservice to the medical center's fundamental mission of improving the lives of its patients. The university and the medical center will vigorously defend this action in court."

Google also offered a strong rebuttal to the suit but would not answer questions.

In a statement emailed to *RPP*, Google said its use of the limited data set was "legal and was approved not only in compliance terms but also vetted by oversight entities including" UC's IRB, its chief compliance and privacy officers, information security officials, and staff from the university and medical center's legal department.

"We believe our healthcare research could help save lives in the future, which is why we take privacy seriously and follow all relevant rules and regulations in our handling of health data. In particular, we take compliance with HIPAA seriously, including in the receipt and use of the limited data set provided by the University of Chicago," Google said in a statement. ✧

PRIVACY BRIEFS

◆ **The Food and Drug Administration is warning patients and health care providers about cyberthreats from using certain Medtronic insulin pumps, which have been recalled.** Security researchers found vulnerabilities in some Medtronic MiniMed insulin pumps that could enable unauthorized users to connect wirelessly to a nearby pump. This could allow a hacker to alter or stop the insulin delivered to the patient. The specific pumps recalled were Medtronic's MiniMed 508 and the MiniMed Paradigm series insulin pumps. Medtronic wrote in a letter to users that it recommended switching to a different type of insulin pump. In addition, it recommended taking additional security steps, including making sure all devices related to the pump were kept in patients' sight at all times, and monitoring blood sugar levels closely. Read more at https://bit.ly/2L4Ftug.

◆ **The health care industry does not have an accurate picture of the sensitive data it acquires, maintains and transmits, according to the results of a survey conducted by Integris Software.** The survey of business executives and IT decision makers at mid- to large-sized companies found that most organizations expressed overconfidence in their technical maturity. Despite the health care industry's history of stringent privacy regulations, it has the second-largest number of cybersecurity breaches when measured across industries, and the highest exposure per breach in 2018, the survey found. More than half of respondents said they needed to access 50 or more data sources to get a defensible picture of where their sensitive data resides, the survey found, even though 70% of respondents said they were "very" or "extremely" confident in knowing where sensitive data resides. Access the survey at https://bit.ly/2YLyYjj.

◆ **An online database of more than 5 million records apparently belonging to the website MedicareSupplement.com was left open and accessible to the public, according to UK-based security firm Comparitech Limited.** The database appeared to be part of the website's marketing leads database, Comparitech says. Records exposed contained full names and addresses, email addresses, dates of birth, genders, and marketing-related information. Around 239,000 records also indicated interest in a particular area of insurance—for example, cancer insurance. Data was spread around several categories, including life, auto, medical and supplemental insurance. The

PRIVACY BRIEFS

IP address of the database first was accessed on May 10 by public search engine BinaryEdge. MedicareSupplement.com disabled access as soon as it was notified. Get the details from Comparitech at https://bit.ly/2XzGqN2.

◆ **Personal data from more than 645,000 clients of Oregon's Department of Human Services (DHS) was compromised during a January data breach, the agency disclosed.** The number is significantly higher than the number included in the agency's original report in March. The data breach occurred as a result of a Jan. 8 email phishing attempt, according to the department. Nine DHS employees opened the email and clicked on the phishing link, giving the scammers access to their email accounts. The compromised accounts were secured by Jan. 28, the department said. After discovering the breach, the department hired a team of 70 attorneys and paralegals to read and sort the 2 million susceptible emails. The people whose personal data was compromised will receive 12 months of identity theft monitoring and recovery services, including a $1 million insurance reimbursement policy. Learn more at https://bit.ly/2xuSiVV.

◆ **Senators Amy Klobuchar (D-Minn.) and Lisa Murkowski (R-Alaska) have introduced bipartisan legislation to protect consumers' private health care data in home DNA testing kits, wearable consumer devices such as Fitbits and health data tracking apps.** The legislation, called "Protecting Personal Health Data Act," would address privacy concerns associated with these new technologies by requiring the secretary of Health and Human Services to promulgate regulations for the technologies. "New technologies have made it easier for people to monitor their own health, but health tracking apps and home DNA testing kits have also given companies access to personal, private data with limited oversight," Klobuchar, who is seeking the Democratic nomination for president, said in a statement. She cited reports about a pregnancy app that's selling user data to the users' employers, and about health apps for users battling depression or trying to quit smoking who sell personal details to third parties, such as Google or Facebook, without their consent. Klobuchar and Murkowski noted that current laws governing medical records privacy were enacted by Congress when many of the wearable devices, apps, social media sites and DNA testing companies didn't exist. The legislation would require appropriate standards for consent that account for differences in sensitivity between genetic data, biometric data and general personal health data. The regulations that would be implemented as a result of the legislation, if approved, would allow consumers to access, amend and delete any personal health data that is collected by apps and devices. The legislation also would create a national task force on health data protection that would evaluate and provide input to address cybersecurity risks and privacy concerns associated with consumer products that handle personal health data. Read the release at https://bit.ly/2LEyzv7.

◆ **More than half of all individuals affected by a health care information breach in the past 12 months were impacted by a breach that touched the affected organization's server**, according to an analysis of breach data on the OCR's website. The analysis, performed by security firm Clearwater Compliance LLC, found that 90 health care breaches—affecting more than nine million individuals—were related to servers in some way. Clearwater analyzed critical and high risks facing hospitals and health systems in its database over the past six months and confirmed that servers topped the list of information system components responsible for those risks, with approximately 63% of all critical and high risks being caused by some inadequately addressed security vulnerability. Dormant accounts and excessive user permissions are the top problems causing the highest risks, according to Clearwater. Download the full report at https://bit.ly/2RZzCHe.

◆ **Union Labor Life Insurance experienced a breach involving personal information of around 87,400 patients when an employee fell victim to a phishing attack,** providing the hacker with login credentials. According to the company, which is a subsidiary of Ullico, an employee opened a malicious link in an email that appeared to be sent from a trusted business partner, and which included a link to a spoof of a legitimate file-sharing site, which prompted the employee to enter login credentials. Compromised data included plan member names, addresses, dates of birth, Social Security numbers, and personal health information of individuals and their family members. The account was disabled within 90 minutes of the unauthorized access, and the account was sequestered from the rest of the network. Officials then took steps to prevent further proliferation of the malicious email. Affected individuals will receive two years of free credit counseling. See the breach notice at http://bit.ly/2YG7WcZ.