Report on
Patient Privacy

Volume 18, Number 9 • September 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

In Second HIPAA Settlement So Far This Year, NY Firm That Exposed IQs Pays State $200,000

Just six months after discovering a data breach that violated HIPAA and New York law, a nonprofit organization that serves individuals with disabilities has already agreed to a $200,000 settlement, State Attorney General (SAG) Barbara Underwood announced on Aug. 29.

But the state settlement doesn't mean The Arc of Erie County is out of the woods with the HHS Office for Civil Rights (OCR), which has shown it is willing to collect penalties even when states have already acted, and especially when sensitive information is at issue as it is here.

The Arc acknowledged that, for nearly three years, information—including IQ scores—was accessible online for close to 4,000 of the "most vulnerable New Yorkers," in the words of Underwood.

In a March 9 breach notice, The Arc said a "coding error" resulted in information for 3,700 clients "contained on two spreadsheets stored on its database" being posted on the internet from July 2015 to Feb. 15 of this year. Exposed data consisted of "full names, social security numbers, gender, race, primary diagnosis codes, IQs, insurance information, addresses, phone numbers, dates of birth, and ages." The exposure did not stem from "a malicious attack seeking protected information."

continued on p. 10

$115M Settlement Ties Anthem to Security Upgrades, Certain Staffing, Spending Levels

Among the 31 FAQs the administrator of the new $115 million Anthem Inc. settlement posted on the website for filing claims is the following: "Will the Settlement help protect data stored by Anthem from another data breach?"

Odds are the estimated 80 million Anthem members and former enrollees affected by the breach are more likely to wonder how much of the $115 million they might receive. Spoiler: $50, or several years of credit monitoring and $10,000 in credit remediation, if required.

However, this provocative question is probably top-of-mind for Anthem officials, already chastened by being party to the most expensive data breach settlement in history, and for HIPAA compliance officials at other health plans, hospitals and provider organizations that don't want to end up like Anthem.

But they can learn from the experiences of the nation's second largest insurer. As with a typical HIPAA state or federal settlement with the HHS Office for Civil Rights (OCR), Anthem's class action suit resolution carries with it requirements to shore up the security of its data. These are spelled out in a list of 13 "business practices," but 11 of these are fully or partially redacted.

Still, the Anthem deal, approved Aug. 17, holds some gems in this regard—the plan is required, for example, to triple the amount it was spending on "information

continued

security" when the hacking occurred in 2014-2015, and maintain that level for three years.

In addition, the settlement obligates Anthem to boost future spending as membership increases, and it must provide security reports to the plaintiffs' attorneys for their review.

The world learned of the breach in February 2015 (*RPP 3/15, p. 1*).

But according to a report issued with an earlier Anthem settlement with state insurance commissioners, the breach "began on February 18, 2014, when a user in Anthem's Amerigroup subsidiary opened an e-mail (commonly referred to as a 'phishing' e-mail) containing malicious content. Opening this e-mail permitted the download of malicious files to the user's local system, allowing the Attacker to gain remote access to that computer. Starting with the initial remote access, the Attacker was able to move laterally (across Anthem systems) and escalate privileges (gain increasingly greater ability to access information and make changes in Anthem's environment). The Attacker utilized at least 50 accounts and compromised at least 90 systems within the Anthem enterprise environment including, eventually, the Company's enterprise data warehouse—a system that stores a large amount of consumer personally identifiable information ('PII'). Queries to that data warehouse resulted in access to an exfiltration of approximately 78.8 million unique user records."

The documents indicate that, once the attack was detected, Anthem was able to shut it down within five days. But the damage was done, according to attorneys for the members and former enrollees. They allege that, as a result of the hack, the individuals had "fake tax returns filed in their names, allowing criminals to abscond with their tax refunds, have had bank accounts drained, and have had credit cards or fraudulent loans taken out in their names."

The affected individuals "spent countless hours filing police reports and poring over credit reports to combat identity theft, but new fraud is still being perpetrated against them using the sensitive information taken during the Anthem Data Breach," their attorneys alleged. They also incurred costs "paying monthly or annual fees for identity theft and credit monitoring services. Now that their sensitive personal information (e.g., their Social Security numbers, dates of birth, and home addresses) has been released, they "worry about being victimized throughout the rest of their lives."

A list of alleged security failures was also submitted with the suit.

Three of Anthem's attorneys who negotiated the settlement did not reply to *RPP*'s emails requesting responses to specific questions. An Anthem spokeswoman refused to provide answers or comment generally on the settlement itself, saying the plan was "declining to comment." Anthem did not admit wrongdoing as part of the settlement.

Andrew Friedman, a partner at Cohen Milstein Sellers & Toll PLLC, and co-chair of the firm's consumer protection practice group, co-leads the suit on behalf of the plaintiffs.

The final division of the $115 million hasn't yet been determined, but as provided for in the settlement and clarified for *RPP* by Friedman, amounts would be distributed as follows:

- The plaintiffs' attorneys will receive $31.05 million plus $2 million for "unreimbursed expenses."
- $23 million goes to a firm hired to administer the settlement.
- $17 million is for credit monitoring.
- $15 million is set aside to pay out-of-pocket claims of up to $10,000 per individual.
- $597,500 will be distributed to 105 plaintiffs in amounts ranging from $5,000 to 7,500.
- Approximately $7 million is earmarked for "all those that wanted alternative compensation rather than credit monitoring" of $50 each.

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 hcca-info.org.

To order an annual subscription to **Report on Patient Privacy** ($482 for HCCA members; $554 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.

◆ Approximately $4.6 million will be available to pay for "another two years of credit monitoring."

◆ Unspecified additional funds "to make up any shortfall in out-of-pocket claims (if there are more than $15 million in valid claims made) and any remaining funds after that pay for even more credit monitoring on a month to month basis."

◆ If funds remain, the Electronic Frontier Foundation and Purdue University's Center for Education and Research in Information Assurance and Security could receive up to $417,000.

To take advantage of the settlement, individuals need to "opt in" by filing a claim. (For more details, including court documents, see http://www.databreach-settlement.com).

Security Changes 'Most Important' Suit Result

"We are very pleased that the court approved the settlement of this case," Friedman tells *RPP*. "We believe the benefits of the settlement, including years of credit monitoring, fraud resolution services, payment of out-of-pocket costs and the business practice commitments, are an excellent result for members of the class."

Friedman calls the case "groundbreaking."

"The settlement, which represents the largest recovery for consumers in any data breach case to date, was groundbreaking in the relief it afforded the class members. It will provide a minimum of four years of triple credit bureau credit monitoring, a minimum of four years of fraud resolution services—even for those persons who do not submit claims) and significant changes to Anthem's data security going forward," he tells *RPP*.

RPP also asked Friedman to innumerate any compliance lessons that other CEs and BAs could take away from this situation.

"Companies that compile personal information on their customers should reconsider what personal information on customers they actually need to retain and should regularly purge unnecessary data," Friedman says. "Moreover, companies should continually review and update their data security and ensure that monitoring systems in place are constantly implemented and reviewed."

Friedman addressed a question from *RPP* about the long-term impact of the suit on preventing hacking and whether breaches were inevitable.

"While hacking attempts may be inevitable, we do not believe that data breaches are," he says. "Material changes to cybersecurity such as has been achieved here, should reduce the chance of future hacks and lessen the severity of hacks, should they occur."

Freidman also defended the redactions in the list of security upgrades.

"There are very compelling reasons not to publish all the details of the business practice commitments," he says. "Among other things, a detailed description of exactly what the security upgrades were would have alerted potential hackers of existing vulnerabilities and, likewise, would have given those same would-be hackers a better chance to successfully circumvent the improved security procedures."

He calls the security upgrades "perhaps the most important benefit" to members.

"Anthem will be required to make or maintain for three years very specific changes to the manner in which it secures class members' personal information," Friedman says. "These measures were derived in consultation with security professionals based upon plaintiffs' extensive discovery. And, to ensure that Anthem maintains enhanced security measures, and that those measures are operating effectively, Anthem will be required both to retain independent consultants to undertake an annual IT security risk assessment and an annual settlement compliance review, and to provide the results to plaintiffs' counsel for review."

The settlement provides "funding for plaintiffs to hire a cybersecurity expert to also review Anthem's reports to insure the enhanced security measures are in place," he added.

Requirement to Shed Data

The actual dollar amount Anthem is to expend on information security is specified—but redacted. In addition, the settlement calls for Anthem to "increase information security spending by [amount redacted] for every additional 5,000 users if Anthem increases its users by more than 10%, whether by acquisition or growth."

Among the aspects of the breach for which Anthem was criticized was that it held onto member data much longer than necessary, given that it still had records on 79 million people when its active enrollment was significantly less.

Based on the unredacted portions of the business practices laid out in Exhibit 2 of the suit, Anthem agreed to "complete deployment" of two steps related to how long it keeps data found in two separate locations or entities, retaining some portion or percentage of both, and then archiving data once it reaches an unspecified age.

Archived data will be protected through "strict access requirements and reviews" and subject to evaluation "on an annual basis to determine what can permanently be removed from the system based on retention requirements." Access to some of the data is permitted only after "additional levels of management approval."

The settlement specifies that sessions "will be automatically terminated after [redacted]" and "users must submit new access requests if access is needed beyond" expiration.

One requirement is standard—or should be—for CEs and BAs, namely, to "annually undertake an annual IT security risk assessment using an outside third party." But the agreement also puts Anthem on a schedule to address findings, something other organizations could consider. Anthem must "remediate 85% of critical and 80% of medium/moderate risk information security audit findings within 2 years and shall remediate 95% of critical findings within 3 years."

Penetration testing and simulated hackings are commonly recommended compliance activities, though few organizations engage in them as often as they should. Under the settlement, Anthem won't have that option.

"Anthem shall conduct adversarial simulations at least twice per year for the [three-year] Settlement Term," Exhibit 2 states. "These simulations, performed by [redacted] will mimic a malicious attacker with internal access to Anthem's network."

According to the settlement, Anthem built a "6000 sq. ft. state of the art Cyber Security Operations Center" (C-SOC) in Indianapolis, which is "staffed 24x7x365 to provide comprehensive monitoring of servers and other technologies to identify improper use of data. The C-SOC's analytic capabilities are employed to detect, analyze and respond to potential security events that threaten the security of data. Anthem shall continue to operate the C-SOC 24x7x365."

Further, staffing is to be maintained. "From 2015-2016, 70 additional information security staff members were hired, including C-SOC team members. Anthem shall keep staffing in place," the documents state.

Contact Friedman at afriedman@cohenmilstein.com. ✧

California's New Privacy Law Sweeps Up Data Common Among Businesses

A sweeping new privacy law approved by California legislators doesn't directly cover protected health information (PHI), but analysts say it will have significant effects on how health care businesses collect, use and store personal data.

The law, approved in a rush in late June to ward off a California ballot initiative on privacy, applies to all for-profit business entities in the state that meet one or more of these criteria: 1) have annual gross revenues greater than $25 million; 2) buy, receive, sell, or share personal information on more than 50,000 state residents per year; or 3) derive 50% or more of annual revenues from selling personal information.

The new law does not apply to nonprofits, including nonprofit health care organizations operating in California. It also does not apply to smaller health care organizations, providing they don't make the majority of their money selling personal information.

However, larger health care organizations that meet the law don't get a pass. Although PHI collected by HIPAA covered entities (CEs) and business associates (BAs) is excluded, other personal information—for example, IP addresses and website usage data collected when a patient visits an entity's website—is covered, says Rachel Marmor, a New York City-based attorney with Davis Wright Tremaine LLP who focuses on data privacy and cybersecurity issues.

"Also, employees are consumers under the law, and any employee data collected by HIPAA Covered Entities [CEs and BAs] would be covered. In short, these entities are still going to be impacted by the law," Marmor tells *RPP*.

The law won't take effect until 2020, and the requirements may undergo some changes prior to that effective date. However, it's sweeping enough that health care organizations should stay on top of it, and know what changes they need to make in order to comply, experts say.

The California Consumer Privacy Act of 2018 (CaCPA) comes at a time when multiple states are focusing on augmenting their consumer privacy statutes (*RPP 7/18, p. 1*). It allows for up to $7,500 per violation in civil penalties and provides consumers with monetary awards for damages.

Similarities With GDPR

The law also provides state residents with more control over their personal information, requiring businesses to tell consumers what's being collected, and give them the right to request deletion of their information and to prohibit businesses from selling it.

"The CaCPA is broader than existing federal and state laws in a number of respects," says Marmor. Laws in effect today, for instance, protect certain narrow categories of information that are considered particularly sensitive, including Social Security numbers and health information, she says.

The new legislation, meanwhile, "protects any information that is capable of being associated with a consumer or household, regardless of whether it is sensitive or what the risks of disclosure are," Marmor says. "This includes name and email address as well as IP address, biometric information, and inferences drawn to create profiles."

The legislation shares some similarities to the requirements in the European Union's General Data Protection Regulation (GDPR), for which the compliance date was May 25 (*RPP 5/18, p. 1*).

Like GDPR, CaCPA similarly has a fairly broad definition of personal information, Marmor says. "But the difference between GDPR and CaCPA in this regard is that whether something is personal information under GDPR is often a contextual test that looks at the ability of the company to link it to an actual person, whereas under CaCPA, a number of fields of data are per se personal information regardless of whether the company ever does or could identify the name of the individual to whom it relates."

Marmor continues: "The key obligations of the CaCPA—opt-out rights, notice requirements for access to data, and right to erasure—are unparalleled in other state laws. While some states now have laws that require companies to adopt appropriate measures to secure personal information—under the narrowed definitions—most state laws focus only on requirements to notify after a breach has occurred."

Act Now, Despite Chance of Amendments

Lawmakers are likely to make at least minor changes to the law to correct obvious typographical errors. In addition, the California attorney general's office has written to legislators suggesting the need for amendments in order to accomplish the necessary rule-making to implement the law, and the business community has backed more substantive changes that are opposed by consumer privacy advocates.

"The range of businesses that will be impacted is broad," Marmor says. "But in particular, businesses that use AI [artificial intelligence] in their operations—for example, to predict patient outcomes or for diagnosis purposes—could face significant challenges."

If these businesses rely on obtaining data from other entities, they may find it more difficult to do so, she says, adding, "businesses may also find that they are facing requests for deletion of data that impact the quality of the data sets being used in AI."

More generally, Marmor says, "health care companies that operate in multiple states are likely to face great operational difficulty in determining which of their consumers are California residents for the purpose of effectuating consumer rights."

This may not be a simple task, she adds: "California law includes in its definition of residents people who are in the state temporarily, as well as people who are domiciled in the state but are temporarily absent."

Health care entities that are affected by the law should start preparing now, Marmor says, even though regulators still haven't begun the rule-making process, and the state legislature still may decide to enact changes to the hastily approved law.

"Businesses will need to have a detailed understanding of what data they possess and where it is stored," she says. "The data mapping required is much more detailed than what would need to be done for the GDPR. Companies should conduct gap assessments and start the process of mapping their data as soon as possible, as these efforts could take months and likely will be needed regardless of any possible amendments to the law."

Businesses that engage in research and clinical trials also need to be cognizant of the potentially negative impacts the CaCPA might have on them, Marmor says.

"Research data necessarily needs to be shared widely in order to analyze and validate the studies—and in some cases, it may not be possible to structure the sharing so as to avoid the consumer's right to opt out," she says. "The law also defines de-identified data in such a way that it's difficult to see how any data sets could be de-identified and still be useful to data analysis, which will further complicate research and predictive analyses by health care companies."

Read the text of the CaCPA at https://bit.ly/2z68PCO. Contact Marmor at rachelmarmor@dwt.com. ✧

When Junking Equipment, Devices, Remember That ePHI Will Live On

A few years ago, a medical device researcher bought a pacemaker and related equipment on eBay. Not only did he acquire the device and its controller, says his friend Rebecca Herold, he also got "very detailed patient data of 51 patients…even including doctors' notes about patient visits and evaluations."

Herold relates the experience in light of a recent monthly newsletter issued by the HHS Office for Civil Rights (OCR), "Guidance on Disposing of Electronic Devices and Media." OCR advises that "organizations should consider whether their process for disposing of electronic devices and media does so in a secure manner."

Obviously, whoever had the pacemaker before her friend didn't do the right thing when it comes to erasing electronic protected health information (ePHI).

OCR's message is one that covered entities (CEs) and business associates (BAs) need to hear, says Herold, president of the HIPAA consulting firm SIMBUS360 and CEO of The Privacy Professor.

Not all CEs and BAs are handling disposal appropriately, and there's sometimes "a mix within the specific organization itself," she tells *RPP*.

Herold says some "do a very good job with disposing of their organization-owned laptops, but then completely overlook the disposal, or decommission, of the laptops that are owned by employees and contractors that are used for business purposes."

The issue is reflected in the quality of entities' plans for disposing of data and media, which Herold says "vary greatly."

While some "have disposal procedures that are multiple pages long and address every type of device and media where data is found," she says, "others simply don't have a documented procedure at all."

And such devices are numerous: think of "desktops, laptops, tablets, copiers, servers, smart phones, hard drives, USB drives," reminds the July OCR newsletter, which was issued in early August.

OCR makes the point—a common refrain from the agency—that a thorough risk assessment is an essential first step in compliance.

Such an analysis "plays a critical role in determining how best to protect data stored on electronic devices and media that has reached the end of its useful life," it says.

The agency offers a list of questions to "consider" when developing strategies to "reduce the risk of breaches of data stored on devices or media scheduled for final disposition:"

◆ "What data is maintained by the organization and where is it stored?

◆ Is the organization's data disposal plan up to date?

◆ Are all asset tags and corporate identifying marks removed?

◆ Have all asset recovery-controlled equipment and devices been identified and isolated?

◆ Is data destruction of the organization's assets handled by a certified provider?

◆ Have the individuals handling the organization's assets been subjected to workforce clearance processes and undergone appropriate training?

◆ Is onsite hard drive destruction required?

◆ What is the chain of custody?

◆ How is equipment staged/stored prior to transfer to external sources for disposal or destruction?

◆ What are the logistics and security controls in moving the equipment?"

According to OCR, when organizations plan for the "final disposition of hardware and electronic media" with ePHI, they should:

◆ "Determine and document the appropriate methods to dispose of hardware, software, and the data itself.

◆ Ensure that ePHI is properly destroyed and cannot be recreated.

◆ Ensure that ePHI previously stored on hardware or electronic media is securely removed such that it cannot be accessed and reused.

◆ Identify removable media and their use (tapes, CDs/DVDs, USB thumb drives).

◆ Ensure that ePHI is removed from reusable media before they are used to record new information."

The newsletter also makes reference to OCR's 2013 document, "Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals."

OCR also provides a list of links that CEs and BAs may find useful, including "Guidelines for Media Sanitization," issued in 2013 by the federal National Institutes of Standards and Technology.

Test to Assure Removal

Calling OCR's advice somewhat "dated," Herold provided *RPP* with a sample data destruction policy (see chart, p. 8). She offers other suggestions for CEs and BAs.

"Establish a process to validate that data was truly completely and irreversibly removed from the digital devices," she says. "Too many times the data wasn't completely removed, and most organizations don't do any testing after going through data removal procedures to ensure the data removal was indeed successful."

Don't forget to address "internet-of-things devices or programs. OCR should have mentioned these," she says, "along with Alexa, Siri and Google Assistant. I have heard from growing numbers of healthcare providers that their doctors and nurses want, or have already started, to use these during patient care and treatment." Says Herold, without OCR opining on these specifically, "I can assure you that at least 90% of CEs will not consider removing data from these devices when it comes to disposing, decommissioning or selling them."

Recycle and resell with care. "Many organizations sell old equipment, often to local used PC/tech stores. This guidance document doesn't mention this—other than includ[ing] a mention of recycling, but that means something different to most people," and officials "assume this only applies to literally disposing of equipment. Selling old equipment in an attempt to reclaim money from an asset is a common practice."

She recommends that organizations' asset management and information security folks both be involved and procedures established and followed to assure data are removed.

OCR advises that organizations ensure "that data privacy is protected via proper migration to another system or total destruction of the data." This statement requires more explanation, says Herold: "Most organizations still consider this to just [mean] destroying the data, but it goes beyond that to ensuring whoever accesses the device before data is irreversibly destroyed does not make copies of the data first, then share it with others."

Pass it on. "Organizations need to make sure their vendors, contractors, and BAs in general have comprehensive disposal policies and procedures in place," says Herold. "It is important for CEs to ensure their BAs aren't creating vulnerabilities to the CEs as a result of their poor disposal practices."

Address employees' personal equipment and devices. Organizations must ensure that PHI is "removed from employee-owned devices before the employee leaves the organization, before they throw it away, give it away, or sell it," she says.

See the OCR newsletter on disposal at https://tinyurl.com/ydhernsh. Contact Herold at rebeccaherold@rebeccaherold.com. ✧

With HIPAA in Mind, Intermountain, Others Usher in Age of Virtual Hospitals

Nearly three years ago, Utah-based Intermountain Healthcare launched its first "virtual hospital," which functions as an advanced form of telehealth for underserved communities. The virtual hospital faces all the same HIPAA privacy and security issues that conventional medical centers and offices face, plus the added challenges that come with managing additional—and constantly changing—processes and vendors for remote electronic connectivity.

In fact, "the development of virtual hospitals and the associated technology stretch HIPAA issues probably to their limit," says attorney Patricia Shea, a partner with K&L Gates LLP in Harrisburg, Pennsylvania.

HIPAA's security rule requires that covered entities (CEs) and their business associates, plus all downstream sub-BAs, perform risk assessments to identify threats and vulnerabilities, and to update those risk assessments and revise the management plan whenever there's been a change to the system, Shea tells *RPP*.

"The biggest pitfall I see is maintaining a current risk assessment and management plan," Shea says, emphasizing "current."

Doing so "is a resource-intensive operation," she says. "To make matters even more critical, OCR [Office for Civil Rights] has repeatedly explained that it views the risk assessment and risk management obligations as extremely important. I advise my clients that this will be, if not the very first thing, at least one of the first things OCR would request during an audit or in response to a 'bad event.'"

As telehealth becomes more sophisticated and more virtual hospitals open, the risk assessment and management process becomes extremely complicated, Shea says, adding, "the numbers of connections and the people involved grow exponentially. I think this aspect of HIPAA compliance will be challenging for these virtual hospitals because changes happen every day. Changes could be in the form of new functionality, the addition of new sites and personnel, the need for new training. It's like a spiderweb of connections."

She adds that "encryption in transit and at rest is a must. This will not eliminate risk, but not doing so in this day and age is likely hard to excuse."

Consider Vendor Indemnification Clauses

Virtual hospitals also need to consider the nature of their relationships with the CEs they serve, Shea says. "The virtual hospitals should get some concrete assurances from these covered entities as to their compliance with HIPAA's requirements. These assurances should have some teeth. If their system is going to be accessing or otherwise connecting to the virtual hospital system, you do not want them to be infecting it."

Shea notes that this would be a factor in the risk assessment and should be addressed appropriately.

A virtual hospital should employ a full-time dedicated information technology staff that's well-equipped to pinpoint problems quickly, according to Shea.

"As new technology emerges and new risks are identified—e.g., new malware and ransomware attacks—holes are going to need quick attention and patching," she says. "This will be a constant," and "training will also be a constant to address changes and newly identified threats."

Applications used by virtual hospitals must be HIPAA-compliant, of course, but CEs using them "should also get very robust warranties and representations as well as indemnification provisions in their agreements with these vendors. A comprehensive review of the cybersecurity policies would also be recommended," Shea says.

"Compliance is never done," she adds. "You may have a comprehensive risk assessment, management plan, policies and procedures, training and everything else, but you have to constantly re-evaluate them. I think

continued on p. 9

Sample Electronic Computing and Data Storage Device Disposal Procedure (Excerpt)

Media Type	General Instructions: Re-Use	General Instructions: Destruction
Cell Phones, Smart Phones	The [information security department, the phone manufacturer, or other area appropriate for the organization] responsible for complying with the computing hardware re-use procedure should follow these steps using Company X approved tools: 1. Copy data from the phone that needs to be retained. 2. Manually delete all information, such as calls made, phone numbers. 3. Perform a full manufacturer's reset to reset the phone back to its factory default settings. 4. Contact [the information security department, the phone manufacturer, or other area appropriate for the organization] for proper sanitization procedure for the specific type of phone. 5. Send the sanitized phone to the area with the responsible for dispersing used equipment.	The [information security department, the phone manufacturer, or other area appropriate for the organization] responsible for complying with the computing hardware destruction procedure should follow these steps using Company X approved tools: 1. Copy data from the phone that needs to be retained. 2. Delete all data, apps, and other software from the phone. 3. Destroy the phone using the most appropriate company-approved method, as indicated by the associated manager. Acceptable destruction methods include: physically destroying using hammer/etc., incinerate in a licensed incinerator, [include other options here]. 4. Dispose of remaining hardware parts/pieces by scheduling a time for the [computing hardware management department or other area appropriate for the organization] to pick up the objects.
Copy Machines, Fax Machines	The [information security department, the phone manufacturer, or other area appropriate for the organization] responsible for complying with the computing hardware re-use procedure should follow these steps using Company X approved tools: 1. Copy data from the machine that needs to be retained. 2. Remove all data from memory. 3. Delete and irreversibly erase all data, apps, and other software from the machine. 4. Perform a full manufacturer's reset to reset the router back to its factory default settings. 5. Contact [the information security department, the phone manufacturer, or other area appropriate for the organization] for proper sanitization procedure. 6. Contact [computing hardware management, or other area appropriate for the organization] to arrange pickup for the copy and/or fax machine. 7. The [computing hardware management department or other area appropriate for the organization] will use a company-approved organization to certify all data has been removed, then arrange for the equipment to be taken to the area or entity for re-use.	The [information security department, the phone manufacturer, or other area appropriate for the organization] responsible for complying with the computing hardware destruction procedure should follow these steps using Company X approved tools: 1. Copy data from the machine that needs to be retained. 2. Remove all data from memory. 3. Completely delete and irreversibly erase all data, apps, and other software from the machine. 4. Arrange for removal of the machines by contacting [computing hardware management department or other area appropriate for the organization] to pick up the machines. 5. The [computing hardware management department or other area appropriate for the organization] will use a company-approved organization to certify all data has been removed, then arrange for the equipment to be taken away by an appropriate disposal vendor.

Source: https://simbus360.com/

continued from p. 7
having the operations/professional folks working closely with the technical folks will be crucial in this regard. Moreover, it should happen at each node of the data flow, including the virtual hospitals and the covered entities and business associates they serve."

Intermountain says it pays particular attention to its BA agreements and to its data-sharing agreements, counsels patients on what to expect, and works with employers that want on-site clinics on privacy issues in order to ensure HIPAA compliance.

The health system has 22 hospitals and 1,600 physicians and advanced practice clinicians at about 180 clinics.

In fact, Intermountain Healthcare considers all of its remote services to be part of its "virtual hospital," even though the remote services aren't licensed as a hospital and do not have the primary role for care of inpatients.

"By design, however, we blur the lines, working to best serve our patients by including all our services, when and where they need them," says Dr. Bill Beninati, medical director for Intermountain Connect Care/Pro, the health system's virtual hospital division. "They may be in a clinic, but their primary provider might access telehealth services for higher levels of care."

To Intermountain, telehealth itself as "an extension of what we already do," adds Kyle Finlayson, the system's compliance program manager. "The HIPAA privacy standards we set for our in-person patient visits apply to our virtual ones such as patient identification and ensuring the patient is okay to discuss their care with anyone in the same room or location as the patient."

The health system's standard process for any new project, product or service is to conduct a security review to ensure sensitive and critical data—which includes protected health information (PHI)—are safeguarded during transmission and processing, as well as when it is in storage or at rest, Finlayson says.

Platforms Differ for Urgent Care, Telehealth

Intermountain organized its telehealth/virtual hospital services into two "buckets": Intermountain Connect Care, which is a direct-to-consumer health care service providing mainly urgent care, and Intermountain Connect Care Pro, which encompasses the health system's professional-facing services and links providers from different care settings and specialties.

"Connect Care Pro is designed to extend services and better use resources, providing another layer of support for smaller rural facilities," Beninati says, adding that it enables patients to stay in their communities, and is a way for Intermountain to load-balance resources and increase efficiency.

As part of virtual health, Intermountain included related services, such as patient transfer and transport, Beninati says.

The health system uses a variety of internally developed and vendor tools to connect patients and providers for virtual health care services—primarily audio and video technology, Beninati says.

He adds, "however, we leverage any kind of technology necessary—high-definition cameras, high-quality microphones, superior A/V, remote monitoring, even wearables—so providers can focus on care rather than the technology. All technology is tested, vetted, and employed only after an extensive security and privacy review to ensure HIPAA compliance."

Intermountain Connect Care, the urgent care arm, utilizes a platform developed by American Well Corporation for telemedicine to connect patients with urgent care providers, says Beninati. Intermountain Connect Care can be accessed directly from a phone, tablet or computer through the Intermountain Connect Care app, which is available on iTunes or Google Play.

Intermountain Connect Care Pro, meanwhile, relies on Intermountain's internally developed telehealth platform, says Adam Hornung, executive director, Intermountain Connect Care/Pro.

"Safeguarding PHI on telehealth visits is no different than in our clinics, hospitals or other Intermountain settings," says Beninati, who states that Intermountain's policies, procedures and caregiver training dictate how to handle, transmit and use PHI in a secure way. The organization utilizes secure file transfer, secure email and encrypted flash media, limits printed PHI to prevent data loss, verifies identity prior to disclosure, and only discloses the minimum necessary to authorized recipients, he says.

Top Areas Include Data-Sharing Management

Intermountain considered four specific areas for potential HIPAA issues when developing its virtual services, says Finlayson. They are:

◆ **Data-sharing management responsibilities.** "Virtual visits introduce the possibility of sharing data with telehealth equipment providers and rural caregivers outside Intermountain's health system," Finlayson says. "It was important to ensure proper agreements were put in place, such as BAAs and data-sharing agreements to ensure data-sharing responsibilities of securing, managing data, and breach responsibilities."

◆ **Private employer kiosks.** "Some implementations of Connect Care included providing a kiosk to employers to offer the benefit to their employees," Finlayson says. "One of the challenges was drafting agreements and providing guidelines to employers that would ensure

the employer-provided kiosks were placed in private locations, such as an office, and possibly [adding] noise-cancelling speakers to ensure patient privacy."

◆ **Patient identification and privacy.** "Similar to in-person visits, our providers use patient identifiers to ensure they are speaking to the correct person," Finlayson says. "Patients also sign a user agreement informing them to take appropriate precautionary measures while using Connect Care, such as using a secure, trusted network, not sharing their login information, and ensuring that no one can see or access the patient's account information. Additionally, the provider asks if the patient is in a private location while care is being provided."

◆ **Cultures and results.** "Some Connect Care visits may require the patient to get a test or culture, such as for strep throat," says Findlayson. "Instead of forcing the patient to make another office visit, the patient is directed to an approved pharmacy that can take the culture, process the specimen, and provide the results. One of the requirements for an approved pharmacy is that they need to have a private location—room or office—where the pharmacist could take the culture, talk with the patient, and provide results."

Intermountain Healthcare did encounter some issues surrounding the security of medical records when developing Connect Care and Connect Care Pro, Hornung says, primarily involving connectivity between medical records. The Connect Care app "required a significant amount of collaboration with our technology partner [American Well] to get an automated process to ensure records from their system are uploaded into our" electronic health record system.

Meanwhile, he says, "As we've worked with external partner facilities through Connect Care Pro, ensuring proper documentation in various EHRs has also proved challenging. Our team has done a tremendous amount of work with these partners to develop an automated, secure process for exchanging patient information in and out of our system."

Says Finlayson, "Who data is shared with and how it is shared is paramount. Intermountain's cybersecurity teams performed risk assessments on the equipment and technology to ensure our patients' data was properly secured during transmission, processing and at rest. The privacy team worked with vendors and outside providers to ensure the proper data-sharing agreements were put in place to delineate data-sharing responsibilities."

Joining the virtual hospital trend is Mercy Virtual Care Center in Chesterfield, Missouri, which opened its doors in 2015 to become what it calls "the world's first facility dedicated entirely to care outside its own walls."

The $54 million building became the nerve center for Mercy's existing telemedicine programs, which include Mercy SafeWatch, a virtual intensive care unit program; Telestroke, a telemedicine stroke care program; and home monitoring.

In addition, health care technology company Royal Philips and the Dutch Rijnstate Hospital announced plans earlier this year to jointly develop a virtual hospital.

As virtual hospitals become more mainstream and widespread, they need to stay on top of HIPAA issues to remain compliant.

Shea says, "The rate of change is an issue. New threats and vulnerabilities introduce themselves routinely. The ability to be prepared to quickly evaluate and address them will be key," she says. "I think there are two very basic issues that are at the heart of the matter: knowing the flow of the information, and having up-to-date, comprehensive risk assessments and management plans."

Contact Shea at patricia.shea@klgates.com and Beninati, Hornung and Finlayson via Intermountain spokesperson Lance Madigan at lance.madigan@imail.org. ✧

NY Gets $200K for HIPAA Violations

continued from p. 1

Details of the breach and settlement are found in the SAG's Assurance of Discontinuance with The Arc, a copy of which Underwood's office provided to *RPP*. The assurance states that The Arc admitted to the facts spelled out in the document.

The spreadsheets at issue were titled "Precision Care" and "Allentown Photo List." On approximately Feb. 8, someone whose data was on one of the spreadsheets phoned a member of the New York State Assembly, who relayed the concern to The Arc via voicemail. The Arc apparently took no action until after the individual phoned on Feb. 13. The organization found the publicly available spreadsheets on Feb. 14, disabled the website and "removed all links by Feb. 16."

According to the state, "the webpage was intended for internal use and was supposed to be protected by a log-in requirement," but it had been online since July 2015.

A security firm The Arc hired found that each spreadsheet had been accessed hundreds of times—Precision Care 289 and Allenton Photo List 265—from Jan. 1, 2017. It couldn't go back earlier than 2017 "because the server logs were not available."

The Arc made required public notification of the breach to clients and others on March 9. Five days later, the state began its own investigation.

Specific HIPAA violations cited are the impermissible disclosure, failure to "perform an evaluation in response to operational change compromising the security" of electronic protected health information (ePHI), and failure to conduct a risk assessment. The Arc also violated a state law requiring protections for Social Security numbers.

The Arc officials did not respond to *RPP*'s requests for comment.

The March notice, which is still available online, also said The Arc was "working with a data security firm and various internet search engine providers to ensure removal of any information that might remain available through the internet" and was "conducting a thorough assessment of its data security to ensure there are no additional vulnerabilities."

The Arc promised that it was "taking steps to improve its privacy and data security practices moving forward by reviewing and updating policies, practices, and training," as well as making the appropriate notice to governmental regulators.

As the state put in its press release, The Arc offered "aggrieved clients with a free one-year subscription to LifeLock to protect themselves from identity theft."

Underwood wanted The Arc to do more, however.

In addition to the $200,000 payment, the settlement calls for The Arc to:

◆ implement a corrective action plan requiring a "thorough risk analysis of security risks and vulnerabilities of all electronic equipment and data systems."

◆ "submit a report of those findings to the Attorney General's Office within 180 days of the settlement."

◆ "review and revise its policies and procedures based on the results of the assessment."

◆ "notify the Attorney General's Office of any action it takes."

◆ "provide a written detailed explanation" if it is determined that "no action is necessary."

In the press release, Underwood said the agreement "should provide a model to all charities in protecting their communities' personal information online."

Although SAGs have had the authority to broker such settlements since 2009—primary authority for HIPAA enforcement lies with OCR—few have. New York has been one of the more active states in this regard, along with Minnesota and Massachusetts (*RPP 11/15, p. 3*).

The settlement is New York's fourth HIPAA agreement since 2015, and the second this year alone.

In January, Aetna agreed to pay $1.15 million following its 2017 data breach in which envelopes with clear windows "confirmed" the HIV status of 2,460 individuals; it also settled a related class action suit for $17 million (*RPP 2/18, p. 5*).

In December 2015, University of Rochester Medical Center paid the state $15,000 after one of its nurses gave a medical practice she was joining information on 3,400 patients whom she hoped would follow her to her new employer (*RPP 12/15, p. 12*).

In an echo of this case, in December 2016, a home health agency paid New York $25,000 to settle allegations it violated HIPAA—and state law—when several of its employees jumped to a new agency, taking with them information on clients, who were later phoned (*RPP 1/17, p. 1*).

As noted, OCR could still take action against The Arc. The incident appears on OCR's website that lists "all breaches reported within the last 24 months that are currently under investigation" that affect 500 or more individuals.

While previous OCR agreements may not have involved the disclosure of individuals' names and IQs, other settlements have involved similarly sensitive data such as HIV status. OCR also has a history of executing agreements with organizations that have already faced state sanctions.

Massachusetts Especially Active

In Sept. 2016, OCR reached an agreement for $400,000 with a health system in Massachusetts after one of its hospitals in Rhode Island lost backup tapes for X-rays, contending there was not an updated business associate agreement between the two (*RPP 10/16, p. 1*). The hospital had already paid the Commonwealth of Massachusetts $150,000 for alleged violations of state data laws and HIPAA stemming from the loss.

Earlier this year OCR collected $100,000 from FileFax Inc., a document storage and shredding firm in receivership (*RPP 3/18, p. 4*). The Illinois firm paid the state $30,000 in 2015 to settle allegations of both state laws and HIPAA violations.

In May of last year, St. Luke's-Roosevelt Hospital Center Inc. paid OCR $387,000 following two impermissible disclosures, including one in which an outpatient center employee mistakenly faxed to an employer a patient's medical record containing "HIV status, medical care, sexually transmitted diseases, medications, sexual orientation, mental health diagnosis, and physical abuse" (*RPP 6/17, p. 5*). ✧

PRIVACY BRIEFS

◆ **The National Cybersecurity Center of Excellence (NCCoE) has released the final version of the National Institute of Standards and Technology practice guide to securing wireless infusion pumps.** "Although connecting infusion pumps to point-of-care medication systems and electronic health records can improve healthcare delivery processes, this can also increase cybersecurity risk, which could lead to operational or safety risks," according to NCCoE. "Tampering, intentional or otherwise, with the wireless infusion pump ecosystem can expose [a healthcare delivery organization] enterprise to serious risk factors, such as: access by malicious actors; a breach of protected health information; loss or disruption of healthcare services; and damage to an organization's reputation, productivity, and bottom-line revenue." The guide provides best practices and detailed guidance on how to manage assets, protect against threats and mitigate vulnerabilities. Download the guide or view it online at https://bit.ly/2Nw4aNC.

◆ **A Texas nurse was fired after a toddler at the hospital where she worked tested positive for measles and the nurse posted about the diagnosis online,** according to hospital officials. Texas Children's Hospital in Houston says it's investigating the incident, and that it stopped a nurse from seeing patients after she reportedly posted about a young boy's condition on a Facebook page called "Proud Parents of Unvaccinated Children." The page since has been deleted. Read more at https://abcn.ws/2PgOGxt.

◆ **Cindy Phillippi, an elected official in Adams County, Wisconsin, allegedly installed keylogging software on county systems, leading to a breach of protected health information, personally identifiable information and tax information for 258,000 people over five years.** Adams County says it uncovered "questionable activity" on the county's computer systems in March that triggered an investigation. According to the county, authorities have opened a criminal investigation, and "suspect(s) no longer have any access rights to view the entirety of the Adams County computer network and system." The County Board of Supervisors has begun the process to remove Phillippi from her elected position. View the breach notification at https://bit.ly/2BLavDw and more details on the case at https://bit.ly/2LjgUp3.

◆ **A couple is suing McAlester Regional Health Center in McAlester, Oklahoma, for HIPAA violations following the drowning death of their adopted toddler.** The child's mother, Denise Russell, said the hospital violated HIPAA when an employee contacted her son's birth mother following his accidental death. Russell said the birth mother then harassed and threatened her family. The lawsuit states that the biological mother "consented to the termination of her rights," and therefore should not have been contacted. The hospital, which denied the allegations, said its "conduct was neither extreme or outrageous." Read more at https://bit.ly/2wp4iY4.

◆ **UnityPoint Health in Des Moines, Iowa, says a data breach could affect 1.4 million patients in both Iowa and North Carolina following a series of phishing attacks disguised as emails from an executive within the organization.** The organization says that it discovered the attack on May 31, and that patient information, including names, addresses, dates of birth, medical information and insurance information, was compromised in the incident. As a result of the attack and investigation, UnityPoint says it has reset passwords, conducted additional training, added technology to identify suspicious external emails, and implemented multifactor authentication. See the breach notification at https://bit.ly/2MyZQRh.

◆ **Another phishing attack led to a breach involving 38,000 patient records at Legacy Health in Portland, Oregon.** The nonprofit health system said it learned in June that "an unauthorized third party may have gained access to some employees' email accounts in May 2018." The subsequent investigation determined that some patient information may have been contained in those email accounts, including names, dates of birth, health insurance information, medical information, and in some cases, Social Security numbers and driver's license numbers. View Legacy Health's breach notification at https://bit.ly/2BI5WKl.

◆ **Augusta University Health also reported a phishing attack that may have exposed sensitive health and personal information of about 417,000 people.** The attack occurred last September, but the university said it didn't confirm that data had been breached or learn about the apparent scope of the attack until July 31. The breach involved a phishing attack by an unauthorized user involving the email accounts of 24 university faculty and administrative personnel. Exposed information may have included names, addresses, medical information and insurance information. Augusta University also said it is investigating another, apparently smaller, phishing attack that occurred in July. Get more details at https://on-ajc.com/2nJ6JRl.