Does Walgreens Loss Set a Precedent for Employer Liability for HIPAA Violations?

When the Indiana Court of Appeals released its decision upholding the $1.44 million jury verdict against Walgreens for privacy violations by an employee pharmacist, the press and blogosphere started buzzing about the precedent it was setting — an employer could be held liable for the HIPAA violations of an employee. This was the view espoused by the plaintiff’s attorney, Neal F. Eggeson, in a statement to the Indianapolis Star on Friday, Nov. 14, the date of the decision.

The plaintiff, Abigail Hinchy, had sued Walgreens and its pharmacist, Audra Withers, for viewing her prescription records without authorization and then disclosing the information to her husband, who was a former boyfriend of Hinchy’s and the father of her child, who threatened to use the information in a paternity lawsuit. After contacting the company, Walgreens acknowledged the HIPAA violation to Hinchy and said that it had given Withers a written warning and required her to retake a HIPAA computer training program.

Hinchy sued both Walgreens and the pharmacist. In her complaint, Hinchy alleged negligence and professional malpractice, invasion of privacy and public disclosure of private facts, and invasion of privacy/intrusion against Withers. She alleged the same...
causes of action against Walgreens, under the theory of “respondeat superior,” under which an employer is held responsible for the actions of employees performed within the scope of their employment. Walgreens argued that an employer should not be held liable for acts of an employee who knowingly violated company policy, in this case, HIPAA policies and procedures.

In its decision, the court of appeals cited a number of Indiana cases to explain the concept of respondeat superior. In particular, it focused on when an employee is “acting within the scope of employment when performing work assigned by the employer or engaging in a course of conduct subject to the employer’s control.” After reviewing the case law, the court concluded that “Withers’s actions were of the same general nature as those authorized, or incident to the actions that were authorized, by Walgreens… Hinchy belonged to the same general category of individuals to whom Withers owed a duty of privacy protection by virtue of her employment as a pharmacist.”

The court also explained that for respondeat superior liability to attach “there must also be underlying liability of the acting party,” in this case, Withers. Hinchy sued Withers for her negligence/professional malpractice.

Walgreens also argued that the $1.44 million jury verdict was excessive and based on improper factors. The court cited evidence admitted at trial regarding the damages, and dismissed Walgreens’ arguments because they amounted to a request to reweigh the evidence, which, the court said, does not do when evaluating a damages award. It found the evidence presented sufficient to support the award.

Privacy attorney Adam Greene of the law firm of Davis Wright Tremaine points out, “Even if a plaintiff can demonstrate a violation of HIPAA, a challenge has been showing damages. What remains to be seen is whether the $1.4 million verdict in the Walgreens case leads to similar findings of harm in other state cases, or whether this was a particularly unique fact pattern.”

Employer Liability for Employees Is Not New

According to Jeff Drummond, a partner in the Dallas office of Jackson Walker LLP, employer liability for employee actions when acting within the scope of employment has been around forever, and to conclude that the appeal confirmed that privacy breach victims may hold employers responsible is an “overreach.” The issue in the Walgreens case was whether the employee was acting in the scope of her employment when the employee breached HIPAA and violated company policy. In this case, the jury decided that the employee was, and the appellate court declined to overturn that decision. But, according to Drummond, “in this particular case, the appellate court gave too much credence to the fact that the employee’s wrongdoing (looking at medical records she shouldn’t have looked at) was very similar to activities the employee would take in the performance of her legitimate duties (looking at medical records she should look at); if that’s the case, a waiter stealing a customer’s credit card number would be attributable to the restaurant owner, which doesn’t seem fair.”

Walgreens also argued that the $1.44 million jury verdict was excessive and based on improper factors. The court cited evidence admitted at trial regarding the damages, and dismissed Walgreens’ arguments because they amounted to a request to reweigh the evidence, which, the court said, does not do when evaluating a damages award. It found the evidence presented sufficient to support the award.

Privacy attorney Adam Greene of the law firm of Davis Wright Tremaine points out, “Even if a plaintiff can demonstrate a violation of HIPAA, a challenge has been showing damages. What remains to be seen is whether the $1.4 million verdict in the Walgreens case leads to similar findings of harm in other state cases, or whether this was a particularly unique fact pattern.”
Drummond points out that “while the pharmacist definitely ‘used’ PHI improperly by accessing PHI she should not have accessed, the plaintiff’s damages came not from that use, but from a further ‘disclosure’ of the data” to Withers’ husband, the father of Hinchy’s child. While the pharmacist’s improper use of the PHI closely tracked the pharmacist’s proper uses of PHI, any disclosure (which would be required for the damages to occur) would not be within the pharmacist’s normal employment activities and might provide a good argument that the actions of the pharmacist were outside the scope of employment.”

Walgreens plans to appeal the court of appeal’s decision.

What Is the Impact on Other State Cases?

So how much impact will this decision have on other state cases alleging privacy violations using HIPAA as the standard of care? Are employers now more likely to be held liable for employees who violate HIPAA while on the job?

According to Drummond, “I don’t think there were too many plaintiffs sitting on the sidelines, not making legitimate state-law claims because they know there’s no private cause of action under HIPAA. I’ve thought all along that, while clearly you can’t sue for a HIPAA violation, you could still sue for a state law violation. These cases may make plaintiffs’ lawyers more interested in bringing marginal cases, where there’s no clear state law allowing a breach of confidentiality claim. But where there’s a clear state law right to sue, I don’t think HIPAA’s ‘no private cause of action’ standard has been much of an impediment,” even before the Walgreens case.

Covered entities, Drummond says, should “have strong, consistent, and enforced policies and procedures. Draft clear data use and disclosure rules and information pathways, and constantly remind your employees of their duties and obligations. Regularly audit your employees and their data access/use/disclosure activities, and encourage your employees to keep tabs on each other (to positively reinforce data rules, but also to report suspicious activities). Promptly correct errors and mistakes, and punish employees who willfully or carelessly violate policies and procedures. Covered entity employers must take visible steps to place HIPAA-violating activities outside the ‘scope of duties’ of their employees in any way they can.”

The case is Walgreen Co. v. Hinchy, No. 49A02-1311-CT-950 (Ind. Ct. of Appeals, Nov. 14, 2014). Contact Drummond at jdrummond@jw.com and Greene at AdamGreene@dwt.com.

Conn. Supreme Court Allows HIPAA To Be Used as a Standard of Care

The state Supreme Court of Connecticut has ruled that a patient may sue a provider for negligence using HIPAA as the standard of care. The Nov. 11 decision by the state’s highest court asserts that “neither HIPAA nor its implementing regulations were intended to preempt tort actions under state law arising out of the unauthorized release of a plaintiff’s medical records.”

This decision joins a line of other state decisions holding that, while HIPAA may not be used to bring a private action against a provider, it may be used to establish the standard of care a provider must meet in actions under state law alleging negligence in terms of protecting the confidentiality of medical information.

In the Connecticut case, the lower court had dismissed plaintiff Emily Byrne’s negligence lawsuit because HIPAA has no private right of action and thus preempts state law claims for negligence and negligent infliction of emotional distress against a health care provider who allegedly breaches the confidentiality of a patient’s medical records to comply with a subpoena. The lower court rejected Byrne’s claim that she was not using HIPAA as the basis of her cause of action, but as evidence of the appropriate standard of care for claims brought under state law. According to the Supreme Court, the lower court said that “plaintiff has labeled her claims as negligence claims, but this does not change their essential nature. They are HIPAA claims.”

Byrne had sued Avery Center for Obstetrics and Gynecology, seeking damages for negligence and negligent infliction of emotional distress after it released her medical records to comply with a subpoena. The lower court rejected Byrne’s claim that she was not using HIPAA as the basis of her cause of action, but as evidence of the appropriate standard of care for claims brought under state law. According to the Supreme Court, the lower court said that “plaintiff has labeled her claims as negligence claims, but this does not change their essential nature. They are HIPAA claims.”

Byrne had sued Avery Center for Obstetrics and Gynecology, seeking damages for negligence and negligent infliction of emotional distress after it released her medical records to comply with a subpoena. The lower court rejected Byrne’s claim that she was not using HIPAA as the basis of her cause of action, but as evidence of the appropriate standard of care for claims brought under state law. According to the Supreme Court, the lower court said that “plaintiff has labeled her claims as negligence claims, but this does not change their essential nature. They are HIPAA claims.”

To Be Used as a Standard of Care

Covered entities, Drummond says, should “have strong, consistent, and enforced policies and procedures. Draft clear data use and disclosure rules and information pathways, and constantly remind your employees of their duties and obligations. Regularly audit your employees and their data access/use/disclosure activities, and encourage your employees to keep tabs on each other (to positively reinforce data rules, but also to report suspicious activities). Promptly correct errors and mistakes, and punish employees who willfully or carelessly violate policies and procedures. Covered entity employers must take visible steps to place HIPAA-violating activities outside the ‘scope of duties’ of their employees in any way they can.”

The case is Walgreen Co. v. Hinchy, No. 49A02-1311-CT-950 (Ind. Ct. of Appeals, Nov. 14, 2014). Contact Drummond at jdrummond@jw.com and Greene at AdamGreene@dwt.com.
reviewed the medical file, alleging “she suffered harassment and extortion threats” as a result.

The state Supreme Court reviewed the issue of whether HIPAA preempts state law claims for negligence and negligent infliction of emotional distress against a health care provider who is alleged to have improperly breached the confidentiality of a patient’s medical records in the course of complying with a subpoena. It pointed to commentary in the original privacy rule, where HHS stated “the fact that a state law allows an individual to file [a civil action] to protect privacy does not conflict with the HIPAA penalty provisions.”

The court then went on to say if the state’s common law recognizes claims arising from a health care provider’s alleged breach of its duty of confidentiality in the course of complying with a subpoena, “HIPAA and its implementing regulations do not preempt such claims....To the extent it has become common practice for Connecticut health care providers to follow the procedures required under HIPAA in rendering services to their patients, HIPAA and its implementing regulations may be utilized to inform the standard of care applicable to such claims arising from allegations of negligence in the disclosure of patients’ medical records pursuant to a subpoena. The availability of such private rights of action in state courts, to the extent that they exist as a matter of state law, do not preclude, conflict with, or complicate health care providers’ compliance with HIPAA.” The court did not reach the issue of whether state common law recognized the negligence claim for breach of confidentiality in the course of complying with a subpoena. Emily Byrne v. Avery Center for Obstetrics and Gynecology, P.C., SC 18904 (Nov. 11, 2014).

Other State Courts Have Recognized HIPAA

Use of HIPAA as the standard of care in state negligence cases has not become the norm, but some state court actions allowing HIPAA to serve as the standard of care have surfaced as attorneys look for ways to press claims for failure to protect an individual’s health information. In 2013, an Indiana jury levied a $1.44 million judgment against Walgreens for failing to protect one customer’s health information. The Indiana Court of Appeals recently affirmed the lower court jury verdict, which would pay $800,000 and agree to a one-year corrective action plan resulting from its ignominious drop-off of 71 boxes of records (RPP 7/14, p. 1). (For a detailed timeline, see story, p. 9).

Most of the time the issue has not arisen in a jury trial but has been presented to the court as the standard to use to measure the defendant’s negligence. State courts of appeal in North Carolina and Utah and the state Supreme Court in West Virginia, as well as two federal district courts in Missouri, have allowed state claims for negligence to proceed using HIPAA as the standard of care.

“While there is no private right of action under HIPAA, this does not mean that courts will ignore the federal law entirely when analyzing whether a defendant acted negligently,” says privacy attorney Adam Greene of the law firm Davis Wright Tremaine.

Connecticut is the latest state to allow the use of HIPAA as the standard of care, and it is the highest state court to make such an explicit ruling. In the Walgreens case, the court of appeals did not address use of HIPAA as the standard of care because Walgreens did not appeal the issue, and the court declined to express an opinion on the recognition of the tort of public disclosure of private facts.

According to Jeff Drummond, partner in the Dallas law firm of Jackson Walker, “in both cases, the issue is whether some common-law or statutory duty of confidentiality was breached, and it certainly appears that it was. The Indiana case is more important for the fact that the employer was held liable for the employee doing something that violated her employer’s policies. Ultimately, whether a particular act constitutes the improper handling of confidential data is going to be determined in light of the requirements of HIPAA, and these cases just make that more clear.”

Health care entities should review state case law and court decisions to see whether there is precedent in their jurisdiction for allowing HIPAA to be used as a standard of care in tort and negligence cases where PHI is involved.

Contact Greene at AdamGreene@dwt.com and Drummond at jdrummond@jw.com.

An Inside Look at OCR Tactics

continued from p. 1

with the health system for privacy rule violations for an amount of money that was significantly less than originally contemplated.

Ultimately it would be another two years after the storage unit visit before OCR would close its inquiry into Hamilton’s wayward files, marking a total of five years almost to the day from when she filed her complaint with OCR. On June 24, 2014, OCR announced that Parkview Health System, Inc., of Fort Wayne, Ind., would pay $800,000 and agree to a one-year corrective action plan resulting from its ignominious drop-off of 71 boxes of records (RPP 7/14, p. 1). (For a detailed timeline, see story, p. 9).

Beyond the obvious messages this case provides for covered entities (CEs) — don’t leave unattended patient files in a driveway, for one — the documents RPP...
reviewed provide a rare inside look into how OCR conducts investigations and the processes it uses to develop a resolution agreement. By paying heed to Parkview’s actions leading up to its decision to leave the files, CEs can also learn valuable HIPAA compliance lessons.

Mix-ups All Along the Way

The arrangement that went so very wrong started out simple enough. In the summer of 2008, Hamilton, of Shipshewana, Ind., had hoped the large hospital system in town would pay for some of her charts, helping her out of a financial fix and providing continuity of care for her patients. In practice for some 20 years, Hamilton met with Ronda Woods, a regional manager for the system, and the two made an arrangement for Hamilton’s files.

In late August Parkview placed ads in local papers saying Hamilton’s office would be closing as of the end of that month and that patients’ files were being transferred to a Parkview physician’s office, and provided that contact information. Parkview also provided Hamilton with a document titled “Agreement to Maintain Records,” which stated that her files would be in three groups. Those patients who wanted to transfer to other physicians were group A; Medicare and Medicaid patients were group B; and the balance were group C. The agreement called for Parkview to buy group C for $10 per chart, but also to “maintain” all of the charts regardless of their group.

The deal began to break down almost immediately, the records show. The date for pickup of the files was changed several times, both sides admit, and neither Hamilton nor anyone else was there on the day in September 2008 when they were taken. According to Hamilton, she put active and inactive files in different rooms, but Parkview contended it was not aware of this. Woods expressed surprise that many files were not in boxes. Even before the pickup, Woods was complaining to Hamilton via email that she did not have an accurate list of charts “for the acquisition.”

By spring 2009, Parkview appears to have been at its wits’ end. Parkview did not believe it had a final chart count and had been receiving patients’ requests for charts it couldn’t find. It even consulted the state attorney general and was reportedly told that office would not get involved.

Woods and other Parkview officials began corresponding with Hamilton, and later her attorney, about returning her records. Both repeatedly told Parkview that Hamilton considered the files to be Parkview’s and that she did not want them back (see related story about PHI ownership, p. 8).

Believing the files were Hamilton’s “ultimate responsibility,” Woods and a handful of other workers brought 71 boxes of files to Hamilton’s home around noon on June 4, 2009. They took this action with the full support of higher-ups at Parkview, OCR would later point out. A week later Hamilton filed a complaint with OCR.

OCR’s investigation took three years to conclude, although, based on the documents, there were long stretches of apparent inactivity. OCR also appears to have been close to ending its investigation as early as 2012. In total, OCR sent three separate data requests to Parkview and made at least one site visit — to the storage unit in May 2012. OCR investigators also conducted phone interviews with Parkview principals involved in the case as well as with the constable for the town where Hamilton had practiced.

OCR Did Its Homework First

According to the documents, OCR did not write to Parkview until it had amassed a great deal of information about the situation, nearly two years after Hamilton first filed her complaint. In April 2011, Celeste Davis, then acting regional manager for OCR Region V, contacted Hamilton by phone. In response, Hamilton provided Davis with copies of photographs of the files in front of her driveway and dozens of emails between herself; Woods; Andrew Rogness, her attorney; Catherine Wilcox, Parkview’s general counsel; and others. She also provided a copy Parkview’s “Agreement to Maintain Records,” which she alone signed.

Davis wrote to Parkview a month later. Revealing nothing of what she had learned from Hamilton, Davis simply summarized Hamilton’s allegation regarding the return of her files and made seven “data requests” of Parkview. Davis asked Parkview for the name of person who would be the agency’s contact throughout the investigation, as well as the names of the individual who “authorized delivery” of the files and who “actually delivered” them, as well as “any written instructions from the former to the latter.” Davis also asked whether all the records taken from Hamilton were returned. In addition she requested a “detailed position statement that responds to Dr. Hamilton’s allegations” along with “any supporting and relevant documentation.”

Additionally, Davis asked for “a copy of your policies and procedures related to safeguarding PHI” as required under section 164.530(c), which requires that a CE “must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.”

The final two requests in the first letter sought information that helps OCR determine the size of any civil monetary penalty or financial settlement. Davis asked for “the number of beds at your facility” and “number of persons served annually.”
Davis’ second letter to Parkview, in which she made 17 new requests for data, was sent in October of that year. These were much more wide-ranging than before and addressed Parkview’s business dealings. She requested, for example, information regarding “potential mergers and acquisitions…for which Parkview reviewed patient medical records” and information about “whether the medical records of the other party were placed in Parkview’s possession or control for its due diligence review.”

She also sought specific details about who within Parkview was involved in each of the various steps regarding the files, including those who negotiated the “potential” purchase as well as who decided Parkview should not go through with it. In addition to names and information about the roles they played, Davis asked whether these individuals were currently employed by Parkview, and for their current contact information.

In response, Parkview sent Davis a 17-page letter with numerous attachments, including a 10-page chart of previous acquisitions. In this correspondence, Ramon Morton, Parkview’s privacy officer, criticized Hamilton as unavailable when problems arose. “After she foisted her medical records mess on Parkview, Dr. Hamilton disappeared on every instance involving her records,” he wrote. Morton also stated that “We believe Parkview was justified in the actions it took. For all these reasons it is Parkview’s hope that OCR will take no further action with regard to this matter.”

That hope, of course, was not to be realized. Davis’ third and final request for data from Parkview was also her briefest. On Dec. 1, 2013, Davis wrote to the president and CEO of Parkview: “OCR is in the process of completing its investigation into this matter and needs additional data,” she wrote. Davis appears to have sought only a “description of the nature of the relationship between Parkview Health System, Inc., Parkview LaGrange Hospital, and Parkview Physicians Group.”

Once received, OCR activity to resolve the case seemed to speed toward its conclusion in earnest. Since the settlement was announced in June, RPP has attempted, without success, to contact Hamilton and learn about the fate of the records. On Dec. 1, RPP spoke briefly to Rogness, her attorney, who said he did not know where she was or what had become of the charts.

RPP submitted questions to OCR about the documents, including why it took five years to close the case, and why the settlement amount had been reduced. “OCR is not in a position to provide additional information regarding our internal investigation,” an agency spokeswoman told RPP in an email.

Perhaps the most revealing among the documents related to the investigation are those that address how OCR decided which regulations were violated, what

---

**PATIENT PRIVACY COURT CASE**

This monthly column is written by Tamara Senikidze of Morgan, Lewis & Bockius LLP in Washington, D.C. It is designed to provide RPP readers with a sampling of the types of patient privacy cases that courts are now hearing. It is not intended to be a comprehensive monthly survey of all patient privacy court actions. Contact Tamara at tsenikidze@morganlewis.com.

❤️ A Louisiana District Court approved a $32.5 million class-action settlement for an alleged unauthorized disclosure of confidential medical records. On October 27, 2014, the Orleans Parish Civil District Court approved the class-action settlement between the plaintiffs and Dallas-based Tenet Healthcare Corp., which owned and operated Jo Ellen Smith Medical Foundation d/b/a Jo Ellen Smith Medical Center and Jo Ellen Smith Psychiatric Center (“the hospital”). The settlement resolved the allegations included in the 1997 class-action lawsuit, that the hospital violated thousands of psychiatric patients’ right to privacy when it improperly discarded boxes of medical records in April 1996. After the hospital closed, the documents, which included patient names and other identifying information, were left in its parking lot, where they were subject to public view and were easily accessible by unauthorized persons. According to the settlement, each class member who files a valid proof of claim can receive a common damages award of $1,000 from the settlement fund. Additionally, class members who suffered personal harm due to the PHI disclosure may be eligible for individual damages payments from the settlement. A court-appointed special master will manage the claims process and recommend appropriate individual damages awards. The special master may also recommend whether heirs of deceased class members could claim damages. Both Tenet Healthcare and the plaintiffs will have the opportunity to object to the special master’s recommendations, and the court will rule in the case of objections. The text of the settlement is available at http://op.bna.com/hl.nsf/id/kcpc-9qcl5/$File/TenetSettle1029.pdf. (John Doe v. Jo Ellen Smith Med. Found.)
penalties to apply and what a corrective action plan (CAP) would entail. The documents show changes over time, likely as a result, at least in part, of negotiations with Parkview. As the number of violations dropped, so did the settlement amounts and the length and breadth of the CAP.

Much of this information is contained in an eight-page document, dated May 14, 2012, titled “Parkview CMP Calculations, Working Draft,” as well as in a resolution agreement submitted nearly two years later to OCR Director Leon Rodriguez for his approval.

The May 2012 working draft pondered sanctions for a total of four violations of the privacy rule. These were:

- “164.530(c) failure to safeguard
- “164.530(i) lack of general safeguards policies and procedures
- “164.530(j) lack of safeguards policies that address due diligence activities” and
- “164.530(e)(1) “failure to possess and/or implement sanctions policies and procedures.”

**OCR Considered Just One of Four Penalty Tiers**

The working draft document, which does not list an author, also contains a table listing the four possible tiers of penalties and their amounts, with “willful neglect not corrected” at the high end. This carries a penalty of $50,000 per violation, with an annual cap of $1.5 million for identical offenses. The other tiers are “did not know,” “reasonable cause,” and “willful neglect, corrected.” They carry penalties of $100 to $10,000 per violation, also capped at $1.5 million per year.

The documents show that OCR later considered just one of these four possible violations, along with another that was not mentioned in the working draft. The resolution agreement approved on April 2 of this year by OCR Director Leon Rodriguez called for action on violations of 164.530(c) and of 164.502(a), which governs “standard uses and disclosures.”

This latter standard was applicable, the April resolution agreement states, because Parkview “impermissibly disclosed” patient PHI by leaving the files on the driveway in an unsecured fashion, “thereby providing the opportunity for someone other than Parkview to access the PHI for a purpose other than permitted by the Privacy Rule.”

The April resolution agreement calculated that “the maximum CMP for all of the indicated violations is $1.55 million.” This was reached based on $50,000 for the safeguards violation and the maximum annual amount allowable of $1.5 million for the impermissible disclosure infraction. OCR concluded that it could levy a penalty of $50,000 for each of the estimated “5,000 individuals” whose records were at issue, an amount that would have been $250 million. However, fortunately for Parkview, OCR also had to apply the $1.5 million cap.

The actual amount specified in this agreement was $1.085 million, “approximately 70% of the total maximum penalty.” The document also pointed out that “the negotiating team from OCR would have the discretion to negotiate this amount downward to $620,000 or 40% of the total maximum penalty.” It called for a three-year corrective action plan.

**Many ‘Aggravating’ Factors**

Although OCR ultimately signed an agreement with Parkview for $800,000 and a one-year corrective action plan based on one violation, OCR did appear to have successfully pressed for the highest level of penalty, willful neglect not corrected.

Technically, the interim final enforcement rule that provides for this did not go into effect until November 30, 2009, and the violation occurred four months earlier, in June of that year. However, OCR had the discretion to apply the higher amount because it was called for under the HITECH Act, which was already in force as of February of that year.

OCR felt Parkview’s actions warranted nothing less, the documents state. “While Parkview’s failure to comply with §§164.530(i) and (j) technically began prior to February 2009, we believe the associated level of culpability should be willful neglect, or reasonable cause at the very minimum,” the working draft states.

Willful neglect, not corrected “applies because Parkview admitted that it left 71 boxes of medical records in Dr. Hamilton’s driveway at time when no one was there to receive or secure them,” the document states. “Parkview’s submission of separate planned and signed delivery statements supports OCR’s conclusion that Parkview’s actions were premeditated [and] that its failure to comply with the Privacy Rule’s safeguards requirement was due to reckless indifference if not conscious intent. Parkview never corrected its violation by retrieving or otherwise security (sic) the record.”

The draft notes that OCR could assess a penalty based on multiple violations of this requirement because there were so many patient files involved, although the $1.5 million cap would ultimately come into play. Unlike other violations more generally, OCR did not view this one as “continuing” but, instead, as a “discrete, one-time event.” Without such a cap, Parkview could have been facing a penalty of $250 million, the documents show.

When there is a continuing violation, the penalties can quickly escalate. OCR can start the clock on a continuing violation from the time the requirement went into effect, with a maximum of six years prior to that
point or from the point at which the CE knew or should have known a violation was occurring but did not correct it.

Under the regulations, OCR considers various “mitigating and aggravating factors” when arriving at a penalty. In this case, the agency listed two aggravating factors for the failure to have safeguards violation — lack of remorse on the part of Parkview and the fact it left “thousands of unattended/unsafeguarded medical records on a residential driveway that is close to a public road and flea market.”

The document notes that OCR had “no allegation or evidence of physical harm caused to patients, hindered ability to obtain healthcare, or financial harm to patients. However, these results could have occurred.”

The financial condition of a CE is another factor OCR considers. In general, OCR wants a CMP or settlement to hurt just enough to call attention to what went wrong and teach others a lesson, but not put the CE out of business.

Here OCR didn’t see an issue that it needed to worry about. “Because Parkview is a large health system, northeast Indiana’s largest healthcare provider (serving a population of 820,000) and one of the region’s largest employers, we do not expect a large CMP would jeopardize its ability to provide health care,” the document states. Parkview did not appear to have had a “history of non-compliance,” which, if present, can be another aggravating factor to support higher penalties.

The internal settlement agreement also includes a section titled, “Policy Reasons to Take the Requested Action.” Here OCR argued that “the nature of the violations of the Privacy Rule reflect an organizational disregard for compliance with the Rule. The indicated noncompliance resulted from a reckless act or failure to act by a manager, officer, executive, or other person of authority within the covered entity,” OCR said. It noted that “Parkview’s Senior Vice President and Chief Operating Officer, Senior Vice President and General Counsel, a Corporate Director and a Regional Manager all participated in the decision to return the medical records at issue, and the Senior Vice President & General Counsel approved Parkview’s delivery of the medical records to Dr. Hamilton’s home.”

---

**Whose PHI Is It Anyway?**

Before employees from Parkview Health, Inc., dropped 71 boxes of a physician’s medical records on her driveway in June 2009 after their deal to buy them had fallen through, Dr. Christine Hamilton and officials of the health system sparred over who owned the charts.

Ten months earlier, Parkview employees had picked up the records from Hamilton’s shuttered office but later concluded the purchase could not go forward due to the “dreadful condition” of the records.

Parkview, of Fort Wayne, Ind., claimed because it did not have a written agreement with Hamilton, the thousands of records were ultimately her responsibility. Hamilton, and later her attorney, contended Parkview owed her money for the records in its possession, and they were not to be returned.

After Hamilton repeatedly refused to name a date and place for Parkview to bring the records, Parkview officials “learned” Hamilton’s home address and emailed her with the details of when they would make the delivery; according to internal OCR documents RPP received after filing a Freedom of Information Act request to HHS (see story, p. 1).

Even when it was being investigated by OCR based on the complaint Hamilton filed, Parkview officials maintained their hands-off stance. In response to OCR’s request for “a copy of your policies and procedures related to safeguarding PHI” as required under the privacy rule, Parkview responded:

“While Parkview Health has multiple policies addressing the safeguarding of protected health information, the medical records in this investigation were the property of Dr. Hamilton. We are not able to provide the policies and procedures followed in Dr. Hamilton’s practice.”

OCR wasn’t buying it. In June OCR announced that Parkview had agreed to $800,000 settlement and corrective action plan stemming from the drop-off (RPP 7/14, p. 1). Parkview and Hamilton’s “contractual dispute” was irrelevant where the privacy rule was concerned, OCR said in the documents RPP obtained.

“Parkview acknowledged that it obtained and/or received medical records from Dr. Hamilton to maintain, transfer and/or purchase,” the documents say. “In doing so, Parkview was required by the Privacy Rule to safeguard the records as long as they were in Parkview’s custody; and until they had been permissibly transferred or destroyed. Parkview’s duty to safeguard the records was not contingent on Parkview entering into a written contract with Dr. Hamilton.”

In settling with OCR, Parkview did not acknowledge any wrongdoing. But the HHS documents reveal...
OCR also predicted the settlement would “send a significant message to covered entities that safeguarding PHI is part of health care providers’ overall implementation of the Privacy Rule.”

The settlement agreement and CAP “will make clear that a health care provider must safeguard PHI as long as the PHI remains in its custody. If the covered entity agrees to the [terms] OCR will publicize this enforcement action, which can be expected to garner substantial media and public interest,” the officials wrote.

**Timeline of OCR Investigation Into Charts Dumped at Doctor’s House**

The fourth resolution agreement for HIPAA violations that the HHS Office for Civil Rights (OCR) announced this year — and likely its last for 2014 — was perhaps its most puzzling: an $800,000 settlement with an Indiana health system that dumped 71 boxes of patient files on a physician’s driveway after attempts to purchase them broke down (RPP 7/14, p. 1).

OCR’s announcement in June said little about the events that led up to the dumping, and nothing about how it arrived at the payment amount.

To learn more, RPP filed a Freedom of Information Act (FOIA) request. Four months later, we received nearly 300 pages of documents and emails related to the case, of “493 responsive records.” The balance of the pages were withheld due to various FOIA exemptions, HHS said.

The clutch of documents chart the five years and 12 days that elapsed from the time Dr. Christine Hamilton of Shipshewana, Ind., submitted her complaint in 2009 to OCR’s announcement of the settlement on June 23 and its letter a month later alerting Hamilton that it had closed her case. Also included is correspondence between Hamilton and Parkview dating back to 2008.

Together they provide a cautionary tale for any HIPAA covered entity that has sought to acquire all or part of another CE, revealing how things can go terribly awry from a HIPAA perspective and otherwise (see story p. 1).

The documents also provide a rare glimpse into how OCR conducts investigations and arrives at settlement terms.

Below is a timeline, pieced together with highlights from these available documents.

- **August 2008:** Dr. Christine Hamilton “approaches” Parkview LeGrange Hospital and Parkview Medical Group “for assistance in closing her practice.” They are part of Parkview Health, Inc. A verbal agreement is reached for payment of $10 per chart for commercial business and public interest,” the officials wrote.

Once it started going through the charts, Parkview had grave concerns about the quality of the PHI they contained. “The documentation in the records did not clearly identify the payer, nor in many instances, the date the patient was last seen by Dr. Hamilton; many chart entries were undated,” Parkview told OCR.

Health system officials were also concerned because Hamilton was still bringing boxes to the physicians’ office where they were being stored, “approximately 25-50 records per box and 1-4 boxes at a time” as late as March 2009. Parkview also complained the only way it had of getting in touch with Hamilton was by email because “she was not answering her telephone and her voice mailbox was full.” Parkview turned to the Indiana Attorney General’s (AG) office but was told their “issue with Dr. Hamilton did not constitute a licensing complaint against an individual over which the Attorney General has jurisdiction to investigate.”

Under Indiana law, the AG is empowered to take possession of “abandoned records.” The documents do not address whether Parkview ever considered this an option.
cial insurance and self-pay patients who, according to Parkview, have been seen in the past two years. Hamilton’s primary contact at Parkview is Ronda Woods, the medical group’s regional manager, who meets with Hamilton in her office.

♦ Sept. 4, 2008: Parkview employees pick up files from Hamilton’s offices. She is not there. In dispute is whether Parkview changed the pick-up date without Hamilton’s agreement and the condition of the files upon pick-up. According to Parkview, the workers, upon arriving, “found hundreds of records lying in stacks on the floor, unboxed, along with boxed records.” Employees couldn’t tell which were active or inactive files, nor what type of payer was identified. Parkview brings the files to two different physicians’ offices for storage and review. Also in dispute is how many files were taken by Parkview. Hamilton says there were 30,000; Parkview says there were 5,000 or less.

♦ September-October 2008: Parkview contends Hamilton is bringing “10 to 25 records at a time” “along with a handwritten list of patient names, dates of birth and payer type” to the Parkview doctor’s office storing the records. Hamilton explains in emails “most” of these files are of women whose babies she recently delivered who she was following until early checks were completed. At this time, Hamilton sends back a signed agreement for maintenance and payment of her records by Parkview. However, health system officials do not sign or return the document to Hamilton, both sides agree.

♦ November 2008: Woods and Hamilton exchange emails regarding incomplete information received about the files.

♦ March 20, 2009: Woods informs Hamilton via email that, due to circumstances occurring in the last seven months with her patient files, the deal is off. Woods gives Hamilton until March 31, 2009, to provide Woods with “a physical address where the records can be delivered.” Woods says Parkview will “box the medical records, maintaining alpha order as we have it” and will make delivery “on a mutually agreed upon data (sic) and time (not to be later than April 30, 2009).” Parkview will keep records “delivered to other physician offices with written request and authorization by the patient.”

♦ March 26, 2009: Andrew Rogness, Hamilton’s attorney, emails Woods to say that “you have already received those files, creating an implied contract” and accusing Parkview officials of being “unjustly enriched by their failure to perform.” Parkview “may not ‘dump’” the files on Hamilton and urging that “you do NEED to have your legal counsel involved….”

♦ March 31, 2009: Catherine Cox, Parkview general counsel, emails Rogness to say that the “offer that Parkview made is withdrawn” because Hamilton’s “medical records are not sufficiently in order to be able to determine the basic facts needed to create the agreement.”

♦ April 21, 2009: Woods emails Hamilton again asking for an address for the files to be delivered.

♦ April 22, 2009: Rogness emails Woods again. “As I indicated in my prior correspondence, Parkview has purchased those files. They should not be returned to Dr. Hamilton!” he writes.

♦ May 28, 2009: Woods emails Hamilton notifying her that “The records will be delivered on June 4, 2009 between 12:00n and 2:00 p.m. to the address mentioned.”

♦ June 4, 2009: Woods and several other Parkview staff pack up the records and drive to Hamilton’s home, trying to reach her by phone and knocking on her door. Woods “senses” someone is home but meets with no one. The Town Constable, Tom Fitch, is called by Parkview. He interrupts his lunch to watch the unloading, but deems the incident not a police matter and does not intervene. The workers leave 71 boxes on the driveway. Hamilton comes home around 4:45 p.m. to find the boxes and calls Fitch back to her home.

♦ June 10, 2009: Hamilton files her complaint online with OCR.

♦ June 22, 2009: OCR notifies Hamilton it has “preliminarily accepted” her complaint, and that “an investigator will contact you in the near future.”

♦ November 2010: An OCR investigator, Felicia Clay, and Hamilton play phone tag for a few days but do not appear to speak to one another.

♦ April 5, 2011: The first successful contact between Clay and Hamilton occurs, based on the records provided to RPP. By letter, Hamilton sends documents to Clay that include photos of the files left at her home.

♦ May 16, 2011: Region V Acting Director Celeste Davis sends her first letter to Parkview. She gives the organization 14 days to respond.

♦ May 23, 2011: Parkview receives the letter and requests an extension to supply the requested information. OCR grants an extension to June 13, 2011.

♦ June 10, 2011: Parkview sends its response to OCR.

♦ Oct. 13, 2011: Davis sends a second data request to Parkview.

♦ Nov. 29, 2011: Parkview sends its response, which includes the statement that “Parkview deeply regrets that this unfortunate situation with Dr. Hamilton developed. The unforceably terrible state of Dr. Hamilton’s records and her unwillingness to take accountability for her records left Parkview in an untenable position.”
◆ May 14, 2012: A document is drafted by OCR or HHS officials titled “Parkview CMP Calculations, Working Draft: May 14, 2012,” which outlines four possible privacy rule violations and associated penalties.

◆ May 31, 2012: An OCR investigator meets with Hamilton in Sturgis, Indiana, at her storage unit. She says the unit contains 8,996 files, both active and inactive. Asked by the investigator to address Hamilton’s earlier estimate that there were 30,000 files, Hamilton tells the investigator 20,000 records were “old but not ancient” and 10,000 were active records.” She “did not know where the other 20,000 might be.”

◆ Dec. 11, 2013: OCR sends Parkview a brief letter asking for “a narrative description of Parkview’s relationship with Parkview LeGrange Hospital.”

◆ March 4, 2014: OCR emails Parkview asking “when the boxes were left on Dr. Hamilton’s driveway, how were the boxes closed or secured (taped, tied, etc….)? Parkview responds that “there were no open boxes” but were secured by “interlocking flaps” or “some other method” and were not “taped or tied.”

◆ March 4, 2014: OCR conducts an interview with Woods, asking her to “walk through” the delivery of the boxes for OCR.

◆ March 31, 2014: Davis sends OCR Director Leon Rodriguez a resolution agreement and corrective action plan, which calls for a three-year CAP and payment of $1.085 million.

◆ April 2, 2014: Rodriguez approves the agreement.

◆ June 17, 2014: Parkview’s CEO, whose name and signature are redacted, and Davis sign a revised resolution agreement. It calls for a payment of $800,000 and a one-year corrective action plan. “This agreement is not an admission of liability by Parkview,” the document states.

◆ June 23, 2014: OCR announces the settlement with Parkview. “All too often we receive complaints of records being discarded or transferred in a manner that puts patient information at risk,” said Christina Heide, acting deputy director of health information privacy at OCR. “It is imperative that HIPAA covered entities and their business associates protect patient information during its transfer and disposal.” The press release calls attention to OCR’s “helpful FAQs concerning HIPAA and the disposal of protected health information.” (See http://tinyurl.com/kzmk2ck.)

◆ June 23, 2014: Owing to the paucity of details concerning what led to Parkview’s actions, RPP submits a FOIA request for all documents related to the case.

◆ July 25, 2014: Davis writes to Hamilton with a copy of the settlement documents, thanking her for filing her complaint.

◆ Oct. 30, 2014: HHS FOIA Privacy Act Division emails 280 pages to RPP.

**PRIVACY BRIEFS**

◆ A hospital chain that the HHS Office for Civil Rights (OCR) believed violated HIPAA by sharing patient information without a signed authorization recently won a lawsuit brought by the patient in California state court. Prime Healthcare Services, parent company of Shasta Regional Medical Center, issued a press release on Nov. 17, stating that it had been “vindicated” in a case brought by Darlene Courtois. A patient of Shasta’s for five days in January 2010, Courtois later shared a 63-page file with California Watch. In response, a Shasta executive met with a news organization and emailed employees details about Courtois’ treatment. In 2012, the health care system was fined $95,000 by the state of California for violating its privacy law and in June of last year it paid $275,000 to OCR to settle allegations of HIPAA violations related to the same incident. However, Prime officials had maintained they acted legally (RPP 7/13, p. 1). According to a news report about the trial, the jury was swayed by the fact that Courtois had already revealed her medical information to California Watch. Courtois’ attorney did not respond to RPP’s requests for comment on whether she planned to appeal. A Prime spokesman told RPP the firm would have no comment beyond the press release, which is available at http://tinyurl.com/ob39zv6.

◆ A patient is suing University of Massachusetts Memorial Medical Center over a data breach by a former employee who improperly accessed patient information and stole several patients’ identities between May 2002 and March 2014, the Telegram & Gazette reported Nov. 24. Robert Jackson and his lawyers are pursuing a class-action lawsuit against UMass Memorial, asking for $3,000 per affected patient and more ID security than the proffered one year of identity theft monitoring. The employee is accused of stealing the identity of 22 people, nine of whom were UMass patients. The hospital said it had notified patients in accordance with state and federal guidelines. Visit http://tinyurl.com/17pr5hx.
PRIVACY BRIEFS (continued)

♦ Beth Israel Deaconess Medical Center in Boston will pay $100,000 over the 2012 theft of a laptop with the unencrypted data of about 4,000 patients and employees, the Boston Globe reported Nov. 22. The hospital was fined for failure to follow policies pertaining to protected health information (PHI) and for the delay in notifying affected patients about the breach. Beth Israel said all of its devices are now encrypted, and employees are also now required to prove their work devices are encrypted on a yearly basis. Visit http://tinyurl.com/mvg5d96.

♦ A laptop and cell phone containing the PHI of 999 patients of Brigham and Women’s Hospital in Boston were stolen in an armed robbery, the hospital said Nov. 17. While the information was protected, the burglars forced the physician to provide them with the passwords to both devices. The devices contained information on patients who were treated at the neurology and neurosurgery centers between October 2011 and September 2014, along with some patients participating in research studies. The data included names, record numbers, ages, prescriptions, diagnoses and treatment information. For more information, visit http://tinyurl.com/kstuqlx.

♦ A glitch put the personal health information of Anthem, Inc. members in the email subject line of preventative screening reminders, Reuters reported Nov. 12. One email subject line read, “[PROOF] - Don’t miss out - call your doctor today; PlanState: CA; Segment: SMALL GROUP; Age: Female Young; Language: EN; CervCancer3yr: N; CervCancer5yr: N; Mammogram: N; Colonoscopy: N.” Reuters said WellPoint declined to disclose how many patients were affected. For more information, visit http://tinyurl.com/om9ptwd.

♦ The American Medical Association announced Nov. 10 it is adopting a new policy to strengthen patient protection. The policy applies specifically to the explanation of benefits (EOB) insurers provide to each primary policy holder. This practice could potentially disclose PHI of other dependents and is of greater importance under the health reform law, AMA said. Members who are dealing with mental health, substance abuse, sexual, reproductive or domestic violence issues are of particular concern. AMA recommended health insurers be required to change EOB listings to prevent disclosure of sensitive information, provide a procedure for all dependents on requesting confidential communication and develop protection for electronic health records. For more information, visit http://tinyurl.com/jwjtkmd.

♦ A missing database server could have compromised the PHI of patients of Visionworks, Inc., a division of Highmark Health, the eye-care chain said Nov. 10. Visionworks said the server went missing during scheduled upgrades and is “believed to have been sent to one of the store’s local landfills.” Credit card information was encrypted, but health information was not. Visionworks will provide customers with free credit monitoring for one year. Visit http://www.visionworks.com/announcement.

♦ More than three quarters of all health care breaches in the past three years were due to loss or theft, according to a Nov. 4 report from Bitglass. Researchers analyzed the list of breaches on the HHS website for the report, finding that loss or theft of medical devices was to blame for 68% of breaches since 2010, while 23% were a result of cyber hacking. Visit http://tinyurl.com/o8b3wxc.

♦ A July data breach at a Miami clinic is currently under investigation by the FBI and the IRS, the health center reported Nov. 3. Jessie Trice Community Health Center said on its website that it was the target of an “identity theft criminal operation” that stole patients’ names, dates of birth and Social Security numbers. Visit http://tinyurl.com/lkr3fv5.

♦ The HHS Office of the Inspector General will review hospitals’ contingency plans in accordance with HIPAA guidelines, it said in its recently released 2015 Work Plan. The HIPAA security rule requires hospitals to have emergency procedures in place in the event of a security breach, OIG said, and it will compare those procedures to government and industry recommendations. For more information, visit http://tinyurl.com/kly4yya.

♦ OCR issued a bulletin in early November entitled “HIPAA Privacy in Emergency Situations” to address how HIPAA applies in circumstances such as the Ebola outbreak. The bulletin addresses the use and disclosure of PHI in emergency situations for treatment, public health activities, disclosures to family and friends, imminent danger and disclosures to the media or others not involved in the care of the patient. Visit http://tinyurl.com/orhonsa.

Call Bailey Sterrett at 800-521-4323 for rates on bulk subscriptions or site licenses, electronic delivery to multiple readers, and customized feeds of selective news and data...daily, weekly or whenever you need it.
If You Don’t Already Subscribe to the Newsletter, Here Are Three Easy Ways to Sign Up:

1. Return to any Web page that linked you to this issue

2. Go to the MarketPlace at www.AISHealth.com and click on “Newsletters.”

3. Call Customer Service at 800-521-4323

If you are a subscriber and want to provide regular access to the newsletter — and other subscriber-only resources at AISHealth.com — to others in your organization:

Call Customer Service at 800-521-4323 to discuss AIS’s very reasonable rates for your on-site distribution of each issue. (Please don’t forward these PDF editions without prior authorization from AIS, since strict copyright restrictions apply.)