Codify
BY AAPC

# Health Information Compliance Alert

## Enforcement News: When HIPAA Trumps State Law Privacy Claims

**Plus: Identity theft hackers could open you up to an investigation by the IRS and FBI.**

Like many other providers, you've been able to rest easy knowing that a specific section in the HIPAA regulations prohibits a private right of action to sue for a HIPAA violation. But some state courts are allowing plaintiffs to use state law claims to circumvent this federal HIPAA prohibition. Has your state jumped on the bandwagon?

**Emily Byrne** sought treatment at the **Avery Center for Obstetrics and Gynecology, P.C**., which provided her with its Notice of Privacy Practices (NPP). Avery's NPP included a description of protected health information (PHI) that the provider could disclose without her authorization in certain circumstances, reported partner attorney **Linn Foster Freedman** in a Nov. 14 analysis for the law firm **Nixon Peabody LLP.**

Byrne specifically instructed Avery not to disclose her PHI to **Andrew Mandoza**, a man with whom she had a relationship. In response to a subpoena from Mandoza in a paternity action, Avery mailed a copy of Byrne's medical file to the court. Avery failed to notify Byrne of the subpoena and didn't file a motion to quash.

Mandoza reviewed Byrne's medical record, and then Byrne moved to seal her medical file. Byrne claimed that she suffered harassment and extortion due to Mandoza's review of her medical records, Freeman said. Byrne filed a lawsuit against Avery for breach of contract (the NPP), negligence, and violations of a Connecticut statute and HIPAA.

The lower court ruled that HIPAA preempted negligence claims under Connecticut state law and that the state law claim was not more stringent than HIPAA. The court stated that HIPAA "preempts any action dealing with confidentiality/privacy of medical information" and that it is "well settled ... that HIPAA does not create a private right of action, requiring claims of violations instead to be raised through the department's (OCR) administrative channels.

**Not so fast:** Byrne appealed the decision to the Connecticut Supreme Court, arguing that although there is no private right of action under HIPAA, she was not asserting a claim for a HIPAA violation  instead, she was asserting common law negligence actions with HIPAA guiding the standard of care, Freeman explained.

The Connecticut Supreme Court agreed with Byrne, noting that it was not deciding whether the state's common law allows a plaintiff relief against a healthcare provider for breaching its confidentiality duty by responding to a subpoena, Freeman said. But assuming that the law does allow this, the court decided that HIPAA does not preempt the action and that federal regulations may inform the applicable standard of care in certain circumstances.

The court decided that neither HIPAA nor its implementing regulations intend to preempt state law court actions stemming from the unauthorized release of a plaintiff's medical records, Freedman noted. "As a result of this holding, Connecticut joined Missouri, West Virginia and North Carolina in chipping away the private right of action preclusion in HIPAA."

**Watch out:** "We will continue to see plaintiffs attempt to argue that state law negligence and privacy claims are not preempted by HIPAA in order to bring claims for data breaches and other HIPAA violations," Freedman warned. "Covered entities and business associates, particularly in the states of Connecticut, Missouri, West Virginia and North Carolina, should take note."

**Beware Of Identity Theft Rings Stealing Your Patient Data**

They might not be looking for medical information, but identity theft criminal rings are aggressively seeking your patients' personal information.

On Nov. 3, Miami-based **Jessie Trice Community Health Center, Inc.** (JTCHC) announced that an identity theft criminal operation stole its patients' personal information. Law enforcement authorities alerted JTCHC of the data breach. The **Federal Bureau of Investigation** (FBI) and **Internal Revenue Service** (IRS) are investigating the breach.

Although the ring did not obtain or compromise any medical records, the theft included 7,888 patients' names, birth dates, and Social Security numbers. JTCHC notified all the affected patients of the data breach and is working with a data-breach response vendor to help their patients.

JTCHC is also "working vigorously and diligently assessing how to mitigate future risks to all patients and has implemented new procedures and protocols to protect patient information so that this type of theft cannot reoccur," President and CEO **Annie Neasman** said in the announcement.

**Could 'Shotgun Pleading' Protect You From Data Breach Lawsuit?**

A "shoddy pleading" could force plaintiffs to redefine their claims against you in a data breach lawsuit, but it won't necessarily win a bid to dismiss the case altogether.

Alabama-based hospital chain **Community Health Systems Inc**. (CHSI) and its subsidiaries filed several motions to dismiss claims arising from a massive data breach that affected 4.5 million patients. CHSI claimed that the plaintiffs' complaints in the lawsuit are classic "shotgun pleadings" and are jumbled, inconsistent, confusing and incoherent, reported Law360.

Patients filed the class action lawsuit against CHSI and its subsidiaries following a data breach earlier this year that allegedly exposed their medical records. In the motions to dismiss, CHSI also argued that it doesn't directly conduct business in Alabama and has a remote role that is too tenuous to trigger personal jurisdiction, according to Law360.

The defendants also argued that only two of the 21 plaintiffs in the case have alleged that they suffered economic loss due to the data breach, Law360 stated. The judge ordered the plaintiffs to respond to the request for a more definite statement of their claims by Dec. 15, 2014, but the court did not yet set a briefing schedule on the motions to dismiss.

**No Electronic Records Causes Sperm Bank Mix-Up**

A woman who underwent artificial insemination with sperm from the wrong donor has filed a lawsuit against the sperm bank  and her claims could impact facilities' recordkeeping and privacy practices.

On Sept. 29, the woman filed a lawsuit against Chicago-based **Midwest Sperm Bank, LLC**, charging claims of wrongful birth and breach of warranty, reported **Britt Killian** in a Nov. 7 blog posting for the law firm **Nixon Peabody LLP.** The sperm bank sent sperm from the wrong donor to the fertility clinic where the woman underwent artificial insemination.

"The media attention surrounding this case largely focused on race-related issues because the plaintiff's articulated losses resulted from receiving sperm from an African American donor rather than the white donor she had selected, with little attention given to the impact this case could have on the operation and oversight of sperm banks in the future," Killian said.

The mix-up occurred because the sperm bank did not keep electronic records, but instead kept hand-written records, the plaintiff alleged. The sperm bank sent the wrong vial to the fertility clinic after one employee wrote the donor's identity as "380" and another employee noted it as "330."

"The court's ruling will likely address the necessity of electronic recordkeeping, privacy protection, and the developing area of law surrounding the professional standards applicable to sperm banks," Killian noted. The **Circuit Court of Cook County, Illinois** is deciding the case.

**Precedent Set: Yes, You Are Liable For Employees' HIPAA Violations**

The **Indiana Court of Appeals** upheld a $1.4-million verdict against **Walgreen** pharmacy chain, potentially setting a national precedent as the first published court decision where a healthcare provider has been held liable for HIPAA

violations committed by its employees.

On Nov. 14, the appeals court affirmed the large jury verdict against Walgreen, reported The Indiana Lawyer. The case involved a Walgreen pharmacist, **Audra Withers**, who allegedly disclosed Abigail Hinchy's prescription history to the customer's ex-boyfriend **Davion Peterson**. At the time, Withers was involved in a relationship with Peterson.

The appeals court agreed with the trial court's verdict, which found Walgreen liable for negligent supervision and retention, as well as invasion of privacy. The fact that Walgreen appealed (and lost) means that courts across the United States can rely upon the verdict in holding employers accountable for their employees' HIPAA violations.