HIPAA Focused Review: Subpoenas and Liability, OCR Enforcement Activity

CTHIMA
August 16, 2019

Presentation by Jennifer L. Cox, J.D.
Cox & Osowiecki, LLC
Hartford, Connecticut

Today's Program

- Subpoenas and Court Orders – dangerous development in Connecticut case law
- Enforcement Activity – analysis of Resolution Agreements over past year
- Q&A

Subpoena Alone – Not Enough

Court Orders, Subpoenas, and Litigation Matters

Connecticut Subpoena Case

The case, *Byrne v. Avery Center For Obstetrics and Gynecology*, involved records disclosed in response to a valid subpoena.

  - Access full opinions at www.jud.ct.gov; Supreme Court opinion archived by date: January 16, 2018.

- Even though HIPAA expressly states it is not grounds for a private right of action, the Connecticut Supreme Court has opined that a common law privacy claim may be based on a breach of HIPAA Privacy.
- Three takeaways:
  - Expect more claims based on HIPAA Privacy or HIPAA breach (although these were already happening)
  - HIPAA is now *de facto* "standard of care" for release of records
  - **BE EXTREMELY CAREFUL** when disclosing in response to a SUBPOENA

Danger Zone: HIPAA and Subpoenas

- ***Byrne v. Avery*** case eventually went to trial. Fact Pattern:
  - October 2004, patient (Byrne) specifically instructed her OB/GYN group not to release her medical record to a particular person (Mendoza).
  - May 2005, Mendoza filed a paternity action against Byrne.
  - Subpoena served on OB/GYN group to appear at a designated office and produce "all medical records" pertaining to the plaintiff.
  - OB/GYN Group mailed a copy of the plaintiff's medical file to the court (probate court).

What's a Subpoena Breach Failure Potentially Worth?

Verdict $853,000

Immediate Lessons Learned

- Do not mail HIPAA-protected records to court as a solution to subpoena (without more careful analysis)
- A lawyer who issues the subpoena – but has not provided an authorization, court order, or satisfactory assurance – and says it's okay to simply mail the records to court is **incorrect**
- Provide that lawyer with the link to a copy of the Supreme Court ruling

Be Very Extremely Careful With Lawyer Requests and Subpoenas!

- Lawyers can subpoena records – but that does not mean you are legally able to comply under HIPAA and/or state law
- **A patient's authorization, court order, or "satisfactory assurances"** are needed before you may release a record in response to a subpoena
- Do not comply with lawyer's subpoena without meeting this rule – best options if you cannot get patient's authorization are motion to quash (or "letter to quash") or seek court order

HIPAA Rules For Judicial And Administrative Proceedings

- You may release in response to an order from a court or administrative tribunal (*but only as much as the order allows – read it carefully*)
- You are allowed to appeal a court order (rare circumstance)
- You will not be held accountable if you choose to comply with a court order, even if the court ends up being wrong
- Other parties might object

HIPAA Rule: Judicial And Administrative Proceedings

Absent an order of, or a subpoena issued by, a court or administrative tribunal, a covered entity may respond to a subpoena or discovery request from, or other lawful process by, a party to the proceeding only if the covered entity obtains either:

(1) **satisfactory assurances** that reasonable efforts have been made to give the individual whose information has been requested notice of the request; or

(2) **satisfactory assurances** that the party seeking such information has made reasonable efforts to secure a protective order that will guard the confidentiality of the information

Satisfactory Assurances

- Satisfactory assurances:
  - If covered entity receives from a requesting party a written statement and accompanying documentation demonstrating that:
    - The party requesting such information has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address); and
    - The notice included sufficient information about the litigation or proceeding in which the protected health information is requested to permit the individual to raise an objection to the court or administrative tribunal; and
  - The time for the individual to raise objections to the court or administrative tribunal has elapsed; and
    - No objections were filed; or
    - All objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution.

Judicial And Administrative Proceedings: Operational Tips

- Have a satisfactory assurance form available if you are going to rely on this
- Keep in mind: most lawyers are not healthcare lawyers and have a low-level understanding of HIPAA, and they think that state litigation rules of practice trump HIPAA (not true)
- Distinguish federal, state and agency subpoenas – complicated rules that may need attorney review
- Some federal agencies have powers to compel disclosure (*e.g.*, Department of Labor in OSHA investigation)
  - ask for citations and paperwork

OCR Enforcement of HIPAA

Resolution Agreements provide a guide to OCR's thought process and enforcement focus

Just Say No To Film Crews

- **September 2018**. $999,000
- Boston Medical Center, Brigham and Women's Hospital, and Massachusetts General Hospital compromised PHI by inviting film crews on premises to film an ABC television network documentary series, without **first obtaining authorization** from patients
- Obtaining consent *after* filming is not enough

Huge Data Loss Results In A Very Hefty Penalty

- **October 15, 2018.** $16 million
- Anthem failed to protect data of 78.8 million individuals from hacking
- Failed to have necessary security systems
- Failed to have adequate system activity review

Repeat Lesson: Do Not Speak To Reporters

- **November 26, 2018.** $125,000
- Allergy Associates of **Hartford**, P.C. released PHI to a reporter in February 2015
- Patient had made a complaint about service animal. A physician-workforce member discussed the issue with the reporter after the complaint was made. Practice didn't discipline the physician.
- OCR's investigation found that the doctor's discussion with the reporter demonstrated a reckless disregard for the patient's privacy rights and that the disclosure occurred *after* the doctor was instructed by group's Privacy Officer to either not respond to the media or respond with "no comment."
- Must also adopt a corrective action plan for ongoing HIPAA compliance

Repeat Lesson: BAA Is Essential For Vendors That Handle PHI

- **December 4, 2018.** $500,000.
- Advanced Care Hospitalists (ACH), a hospitalist contract/staffing service, working in Florida
- 2011 and 2012 ACH used a third-party billing company, but **failed to obtain a BAA**
- Billing company was less than professional, failed to protect PHI; hospital came across patient data on open website, informed ACH
- ACH also failed to have BAA policy, SRA, or other basic HIPAA policies

Repeat Lesson: Must Terminate Employee Access When Job Ends

- **December 11, 2018**. $111,400.
- Colorado critical access hospital failed to terminate access rights of an employee for months after separation
- Also failed to have a BAA with scheduling vendor

Failing to Fix Known Errors, Failing to Have Adequate Security

- **February 7, 2019**. $3,000,000.
- Cottage Health three hospitals in California, reported breaches in 2013 and 2015, both relating to improper configuration of servers, allowing access over the internet and without requiring unique ID/password.
- Exposed patient names, addresses, dates of birth, diagnoses, conditions, lab results, other treatment information to anyone with access to Cottage Health's server, and exposed ePHI over the unsecured
  - Failed to conduct accurate and thorough SRA
  - Failed to deploy routine security measures
  - Failed to obtain BAA with vendor

Cover Up (Or An Anemic Response) Can Make Things Worse

- **May 6, 2019**. $3,000,000
- Touchstone Medical Imaging (Tennessee) was informed by the FBI that their server had been accessed by unauthorized entity
- Response to FBI's notice was underwhelming and self-serving, concluding no breach
- In reality, Touchstone failed to: properly recognize issue, provide timely breach notice, or remediate exposure of 300,000 patients' PHI
- Also failed: to have BAAs, to have adequate SRA

Adequate SRA Is Mission Critical

- **May 23, 2019**. $100,000.
- Medical Informatics Engineering (MIE), an Indiana based company, provides software and medical record services to providers
- July 2015, MIE reported breach of 3.5 million patient records – hacking event using compromised ID/password
- OCR found MIE failed to perform adequate SRA prior to breach

Q & A

Other Tools And Resources From OCR

- OCR's focus is revealed in its advisories, tools, and press releases, all of which can be found at: www.hhs.gov/ocr/privacy/

Some specific tools and education areas include:

- Model NOPP (and Spanish Model NOPP)
- Model BAA
- Dangerous individuals
- Mental health records
- Mobile devices de-identification decisions
- Security Rule risk analysis guidance
- Security Rule white papers and NIST links