

HIPAA & Discovery

February 7, 2017

Professionalism & Ethics CLE presentation

Amber Ellis, Assistant Counsel, St. Luke's Health Systems

Amberc.ellis@gmail.com

Official Disclaimer

The information provided in this presentation is for informational purposes only. These slides do not constitute legal advice, nor do they reflect the views of St. Luke's Health Systems or necessarily any of its attorneys. The views expressed herein are solely those of the speaker. There is no implicit guarantee that this information is correct, complete, or up-to-date.



Health Insurance Portability and Accountability Act

- Privacy Rule: 45 CFR 164.500 (2003)
 - Nat'l standards for protection of individually identifiable health info
- Security Rule & Enforcement Rule: 45 CFR 164.300 (2005)
 - Nat'l standards for protecting ePHI
 - Standards for enforcement
- HITECH Act: 42 USC 17921 *et seq* (2009)
 - expanded responsibilities of business associates
 - Penalties for violations
- Omnibus Rules (2013)
 - Breach notification rule
 - Implemented HITECH fully

Covered Entities & Business Associates

- Health care providers who engage in certain electronic transactions
- Health plans, including employee group health plans if:
 - 50 or more participants; or
 - Administered by a 3rd party; or
 - Healthcare clearinghouse

45 CFR 160.103 - definitions

- Business Associates of covered entities.
 - Vendors who use or access PHI as part of providing services to covered entities.
 - Must enter into a Business Associate Agreement BEFORE obtaining PHI
 - Sample BAA on HHS website:
<https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html>

Privacy Rule

- Regulates how CE/BA uses, accesses, and discloses PHI.
- Personal Health Information – any individually identifiable health information. 45 CFR 160.103
- Fundamentally: CE may not use or disclose PHI except:
 - As the Privacy Rule Permits or requires, or
 - As the patient authorizes in writing

Disclosures

- Most disclosures are *permissive*.
- Disclosure *required* only in 2 circumstances:
 - **Individuals** (or personal representatives) when they **request** their PHI records or an accounting of disclosures of their PHI, or
 - **HHS** when it undertakes a compliance investigation or review of enforcement action.
- See 45 CFR 164.502(a)

Privacy Rule, Permissive Disclosures

- A CE may disclose PHI under the following exceptions:
 - as **authorized** by the patient or his/her personal representative in writing, or
 - as allowed by the privacy rule – remember principle of Minimum Necessary 45 CFR 164.502(b) and 164.514(d)
 - Purposes of treatment, payment or healthcare operations
 - Incidental Use and Disclosure
 - Limited Data set – de-identified
 - Safety or Government purposes
 - Military purposes
 - Persons in custody

Privacy Rule, Permissive Disclosures

- Safety or Government Purposes

- Court order
- Workers comp
- Law enforcement in certain circumstances
 - Look to state law
 - Typically, in response to a law enforcement official's request about a victim or suspected victim of a crime
 - coroner
 - domestic violence, violent crime, child abuse
- Public health activities (vital statistics)
- Research
- Health oversight activities
 - Audits investigation

Privacy Rule, Permissive Disclosures

- For disclosures to family and others involved in the patient's medical care or payment for care if:
 - The patient hasn't objected
 - Disclosure is appropriate
 - Limit disclosure to minimum necessary
- **ALERT:** psychotherapy notes require separate and distinct authorization. NOT part of designated record set, separate notes kept by therapist.

PENALTIES

- CIVIL PENALTIES:
- 45 CFR 160.400 (HITECH Act increased)
- Did not know & should not have known: \$100 to \$50,000 per violation. Up to \$1.5 million per type per year. No penalty if corrected within 30 days.
- Willful neglect: MANDATORY penalty of at least \$10,000 per violation.
 - If not corrected within 30 days, MANDATORY penalty of at least \$50,000

PENALTIES

- CRIMINAL PENALTIES:
- 42 USC 1320d-6(a)
- Knowingly obtain info in violation of the law: \$50,000 fine and up to 1 year in prison.
- With intent to sell, transfer or use for commercial gain: \$250,000 fine.

Authorization to disclose to Third Party

- **A description of the information to be disclosed -- specific and meaningful.**
- **The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.**
- **The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure.**
- **A description of each purpose of the requested use or disclosure. The statement “at the request of the individual” is a sufficient description.**
- 45 C.F.R. § 164.508.

Authorization Elements Contd.

- **An expiration date or an expiration event.** The statement “end of the research study,” “none,” or similar language is sufficient.
- **Signature of the individual and date.** If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided.
 - i.e. indication that signatory is a parent, or guardian.

Authorization Elements, contd.

- **The potential for information disclosed pursuant to the authorization to be subject to re-disclosure by the recipient and no longer be protected by this subpart.**
- **The individual's right to revoke the authorization in writing, and either:**
 - **The exceptions to the right to revoke and a description of how the individual may revoke the authorization; or**
 - **To the extent that the list of exceptions to the right to revoke is included in Notice of Privacy Practices, a reference to the CE's notice.**

Authorization Elements, Contd.

- **The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization, by stating either:**
 - The covered entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization when the prohibition on conditioning of authorizations applies; or
 - The consequences to the individual of a refusal to sign the authorization when the covered entity can condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization.
- **Plain language requirement.** The authorization must be written in plain language.

Subpoenas

- A third-party subpoena, standing alone, is **insufficient** to allow a covered entity to disclose PHI.
 - Yes – subpoena is a binding court order. A response or appearance is required, if otherwise valid.
- Requires: *Satisfactory Assurances* that—(1) the patient has been notified of the request or (2) a qualified protective order has been sought. 45 CFR 164.512(e)(1)(iii).

Satisfactory Assurances

- Issuer must provide a WRITTEN statement and documentation showing:
 - The patient was provided written notice of the subpoena (or good faith attempt made)
 - The notice included enough information about the litigation so the patient could object, AND
 - The time for objection has passed and there were no objections OR the court has resolved any objections in a manner consistent with disclosure

Protective Order

- Parties may stipulate or otherwise obtain a protective order that:
 - Prohibits the parties from using or disclosing the protected health information for any purpose other than the pending litigation or proceeding AND
 - Requires the parties to return or destroy all copies of the PHI at the end of the proceeding. 45 CFR 164.512(e)(1)(iv)

Court Order

- A subpoena, court order, or warrant signed by a judge, as opposed to an attorney or a clerk of the court, is sufficient to require disclosure of the PHI
- Minimum necessary principle applies.
- For sensitive patients (minors) often include only initials and partially redacted date of birth – a cover letter including patient identifiers will be necessary to identify patient and disclose records

Subpoena Best Practices

- Attorney seeking PHI, send notice to the patient with a copy of intended subpoena plus instructions on how to object and a deadline
- Include a copy of the notice along with the subpoena to the covered entity
- Include an additional written statement that no objection was received/that any objection was resolved – include any relevant court orders

Resources

- www.healthIT.gov
- www.hhs.gov/hipaa/
 - Sample Business Associate Agreement
 - Tools to assess whether your entity is:
 - A covered entity
 - A business associate
 - Checklists for compliance
 - Training toolkits

Thank You!

