HIPAA Basics

- Who is a “covered entity?”
- What is PHI?
- When can you disclose PHI (TPO)?
- When do you need an authorization?
- How do you handle complaints?
HIPAA Basics

- What is “minimum necessary?”
- Who is a business associate?
- What is a BAA?
- What is a Notice of Privacy Practices?
- How do you handle a breach?
- Who is in charge of HIPAA compliance?
What Does the Final HIPAA Rule Mean for Physicians?

1. Direct liability of Business Associates
   - Failure to comply with BAA related to PHI
   - Failure to provide PHI to HHS upon demand
   - Failure to provide PHI to an individual upon request
   - Failure to make reasonable efforts to limit PHI to “minimum necessary”
   - Failure to enter into BAA with subcontractors
What Does the Final HIPAA Rule Mean for Physicians?

2. Business Associates directly liable for their HIPAA violations

3. Subcontractors are also Business Associates and must sign BAAs

4. Changes to BAA form — must comply by Sept. 23, 2013
What Does the Final HIPAA Rule Mean for Physicians?

5. Enforcement / penalties:

- “Did Not Know” penalty — $100 to $50,000 per violation (would not have known)
- “Reasonable Cause” penalty — $100 to less than $50,000 per violation when reasonable cause and not willful neglect
- “Willful Neglect-Corrected” penalty — $10,000 to less than $50,000 per violation
- “Willful Neglect-Not Corrected” penalty — $50,000 per violation
- Annual maximum $1.5 million
Final HIPAA Rule

What Does the Final HIPAA Rule Mean for Physicians?

6. Prohibition on accepting remuneration for PHI without patient authorization, except under certain circumstances

   • Use of PHI related to psychotherapy, marketing, sale of PHI
   • Right to opt out of fundraising communications
   • Right to restrict disclosures to a health plan where paying out of pocket
   • Right to be notified about PHI breaches
What Does the Final HIPAA Rule Mean for Physicians?

8. Modification to Breach Notification Rule

a) Notify any patient whose PHI has been compromised or breached in a manner that compromises the security and privacy of the patient’s PHI.

b) An impermissible use or disclosure of PHI is presumed to be a breach unless the practice can demonstrate that there is a low probability that the protected health information has been compromised based on the following four factors:
   • The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
   • The unauthorized person who used the PHI or to whom the disclosure was made;
   • Whether the PHI was actually acquired or reviewed; and
   • The extent to which the risk to the PHI has been mitigated.
What Does the Final HIPAA Rule Mean for Physicians?

9. Breach notification

• No later than sixty (60) days from a breach, the practice must provide written notice (via first class U.S. mail or e-mail if the patient has previously expressed a preference for e-mail communication) to the patient whose PHI is subject to such breach.

• In the event contact information for ten (10) or more persons subject to a breach is out of date or incomplete, the practice must post a notice on its website for ninety (90) consecutive days. The notice will provide a description of the breach and a toll-free number for those who may be affected to contact the practice. In no event will any patient-specific information be posted to the website.
What Does the Final HIPAA Rule Mean for Physicians?

• In the event notice to a patient is urgent or of a nature that the patient must be notified immediately, the practice must telephone the patient directly regarding the breach.

• If a breach involves more than 500 patients in a given state or geographic area, the practice must immediately, but in no event more than sixty (60) days from discovery of the breach, notify a local, prominent media market. In addition, practice must notify HHS of the breach contemporaneous with the notice to patients.

• The practice must maintain a log of all breaches affecting less than 500 patients in any calendar year. Within sixty (60) days of the end of the calendar year, the covered entity will notify HHS of all breaches (other than low probability breaches).
What are the most common HIPAA mistakes by medical practices?

• Not executing BAA agreements

• Not implementing the requisite technology safeguards
What are the most common HIPAA mistakes by medical practices?

• Not reviewing state, local requirements
  • Example: Texas HB 300

• Not performing a risk analysis
HIPAA Best Practices for Physicians

• Establish a compliance program
• Understand the potential source of breaches
HIPAA Best Practices for Physicians

• Update BAA Agreements
  • Joint ventures and ACOs
  • Curtail to different vendors
  • Establish relationship (delineate state, federal designations as a covered entity, business associate, or subcontractor)

• Evaluate technology safeguards regularly
For more information:

• eadler@kr-law.com

• rvrose@rvrose.com

• PhysiciansPractice.com/HIPAA