HIPAA and 42 CFR Part 2: What does it have to do with you?

Carolyn Heyman-Layne, Esq.
Covering the Basics

- HIPAA
- 42 CFR Part 2
- Other potential privacy laws: Privacy Act, FERPA, AK PIPA, other State laws
- Other healthcare liability concerns for board members
HIPAA is usually the minimum for confidentiality, and 42 CFR Part 2 is usually the maximum.
The Health Insurance Portability and Accountability Act of 1996 (HIPAA) contains three parts:

- Privacy Rule
  - Who can access medical records and why?
- Security Rule
  - Are the medical records properly and safely stored?
- Transactions and Code Set Standards
  - Are healthcare transactions conducted under the proper standards?
Purpose of Privacy Rule

- To protect the rights of consumers and control inappropriate use of health information
- To improve quality of health care by restoring trust in the system
- To improve efficiency and effectiveness of health care delivery
Quick summary of key concepts:
- HIPAA applies to Covered Entities.
- Covered Entities are required to protect Protected Health Information.
- Uses and disclosures are allowed for treatment, payment and health care operations.
Privacy Rule obligations are imposed only on Covered Entities:
- Health plans
- Health care providers
- Health care clearinghouses

Persons who are not Covered Entities may still be affected by HIPAA

Persons who do not handle health information may still be subject to HIPAA
HIPAA governs the use and disclosure of protected health information (PHI)

PHI is individually identifiable health information (IIHI), written or oral.

PHI excludes information in education records covered by the Family Educational Rights and Privacy Act, and employment records held by a covered entity in its role as employer.
A Covered Entity may use and disclose PHI without patient permission for treatment, payment, and health care operations (TPO).

These terms are broadly defined and can apply to a number of uses and disclosures.
The Privacy Rule generally requires covered entities take reasonable steps to limit use or disclosure to the minimum necessary to accomplish the intended purpose.

Disclosures for treatment purposes or pursuant to an authorization are excluded from the minimum necessary requirements.

Covered entity decides the minimum necessary!
In addition to treatment, payment and healthcare operations, Covered Entities can disclose PHI to Business Associates.

Business Associate: A person other than a member of the Covered Entity’s workforce who performs a function or activity on behalf of a Covered Entity involving the use or disclosure of PHI.
Business Associate Agreements

- It is the responsibility of the Covered Entity to enter into Business Associate Agreements with their business associates.
- Business Associate Agreement can be separate document or included as provision in larger contract.
- Covered Entity may be a business associate, as well as a covered entity.
Provide information to patients about their privacy rights and how their information can be used (Notice of Privacy Practices).

- Adopt clear privacy procedures.
- Train employees to understand privacy procedures.
- Protect patient records that contain IIHI.
- Report breaches of PHI.
The Security Rule was enacted to physically protect health information. Focuses on administrative, physical and technical security of information.

• Administrative: Employee access rights
• Physical: Workstation locations
• Technical: Automatic logoff

HITECH – HIPAA now includes breach reporting requirements.
Security Rule: Administrative

- Conduct Risk Assessment
- Security Management Process
- Assigned Security Responsibility
- Access Authorization
- Termination
- Awareness & Training
- Security Incidents
- Contingency Plans
- Evaluation
- Business Associate Agreements
Security Rule: Physical

- Facility Walkthrough
- Security Plan
- Contingency Operations – can be part of overall emergency response plan
- Maintenance records
- Workstations
- Disposal & Destruction
- Backup & Copy
- Reuse & Recycling of Equipment
- Encryption & Decryption
Security Rule: Technical

- Access controls
- Automatic Logoff
- Termination
- Audit Controls
- Integrity
- Person or Entity Authentication
- Data Transmission
What is a “breach”? 

**HITECH/HIPAA**
- Acquisition, access, use or disclosure of PHI in a manner not permitted under HIPAA, which compromises the security or privacy of the PHI.
- Only applies to “unsecured PHI”, such as unencrypted data on a laptop, etc.

**AK PERSONAL INFORMATION PROTECTION ACT (AK PIPA)**
- Unauthorized acquisition, or reasonable belief of unauthorized acquisition of personal information that compromises the security, confidentiality or integrity of the personal information.
- Only applies to “personal information”: not encrypted or redacted; combination of name and identifying number (SSN, DL#, credit card or bank account, etc.)

Privacy breach insurance is available!!!
## HITECH vs. AK PIPA: Breach Reporting

<table>
<thead>
<tr>
<th>HITECH</th>
<th>AK PIPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only covers unsecured protected health information</td>
<td>Covers “personal information” if reasonable likelihood of harm</td>
</tr>
<tr>
<td>Written notification</td>
<td>Written or electronic notice</td>
</tr>
<tr>
<td>More than 500 affected requires notice to media</td>
<td>More than 300,000 requires notice to media</td>
</tr>
<tr>
<td>Notice within 60 days of discovery</td>
<td>Requires reporting to AG even if no harm caused</td>
</tr>
<tr>
<td>Specific notice requirements</td>
<td>Make sure this is covered in business associate agreements and vendor contracts</td>
</tr>
<tr>
<td>Notice to HHS or annual log of breaches</td>
<td></td>
</tr>
</tbody>
</table>
“Covered Entity” under HIPAA
- Providers
- Health Plans
- Healthcare Clearinghouses

“Program” 42 CFR 2.11
- An individual or entity that “holds itself out as providing, and provides, alcohol or drug abuse diagnosis, treatment or treatment referral”
- Unit within a general medical facility that holds itself out as providing diagnosis, treatment or treatment referral
- Must receive federal assistance
## HIPAA vs. 42 CFR Part 2

<table>
<thead>
<tr>
<th>HIPAA</th>
<th>42 CFR PART 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Covered Entities</strong></td>
<td><strong>Part 2 Programs</strong></td>
</tr>
<tr>
<td><strong>Protected Health Information (PHI)</strong></td>
<td><strong>Information that identifies substance abuser</strong></td>
</tr>
<tr>
<td><strong>Protects medical record numbers</strong></td>
<td><strong>Does not protect medical record numbers</strong></td>
</tr>
<tr>
<td><strong>Allows disclosures without authorization for treatment, payment and healthcare operations</strong></td>
<td><strong>Does not allow any disclosure without consent except in very limited special circumstances</strong></td>
</tr>
<tr>
<td><strong>Business Associate Agreements</strong></td>
<td><strong>Qualified Service Organization Agreements</strong></td>
</tr>
</tbody>
</table>
Applying HIPAA & 42 CFR Part 2

- Apply the law that provides the most privacy and security (usually Part 2)
- Make authorizations/ROIs consistent with both regulations
  - Patient Name
  - Meaningful description of information disclosed
  - Specific name of persons authorized to disclose
  - Name of persons authorized to receive
  - Purpose of disclosure
  - Expiration date/event
  - Right to revoke & how
  - Not conditioning treatment, etc.
  - Part 2 re-disclosure statement
Be careful!

- No patient identifying information – why are you disclosing? Can you do it anonymously?
- Make sure and document disclosures for medical emergencies
- Subpoena alone not sufficient for Part 2, entity can require both subpoena and court order
- Not all required reporting can be done under Part 2 – need consent, anonymous or QSOA
Comment period ended April 11, 2016
Intended to modernize Part 2 and facilitate electronic health records and electronic exchange
Alcohol and drug abuse substance use disorder
Applicability revised re: general medical facilities and general medical practices
Allows general designation of recipient
SAMHSA’s Proposed Part 2 Update

- Consent requires explicit description of substance use disorder treatment information to be disclosed
- Consent requires the disclosing entity to be specified
- Consent must include acknowledgement that patient understands terms
- Patient has the right to list of disclosures if general designation used for recipient
SAMHSA’s Proposed Part 2 Update

- Electronic signature permitted on consent
- Changes for research
- Changes for audit and evaluation purposes
- Security of records enhanced and required of recipients of Part 2 info, not just Part 2 providers
  - Correlates somewhat with HIPAA security
Revised definition and discretion with “medical emergency”

Notices to patients:
- Can be provided in paper or electronic format
- Should include information for reporting violations
- Can be combined with HIPAA Notice of Privacy Practices

Reporting by methadone programs transferred to SAMHSA from FDA
Privacy and New Technology

Texting – Is it HIPAA compliant?

- What are you texting? PHI?
- How are you texting? Secure texting app or regular phone texting?
- How is the text reflected in the patient record?
- Has the patient consented to using texts?
- Can you provide the patient with access to the text record?
- Does the record reveal information about other patients or personal provider info?
- Is the phone encrypted?
Texting – Other Issues:

- Is the disclosure permitted under Part 2?
- Has staff been trained on appropriate use?
- Do you have policies/procedures in place?
  - Allowable use
  - Access to employee owned phones
  - Deletion of PHI
  - Turning on tracking/encryption
- Is there a way to know what PHI is on a phone if it is lost/stolen?
Privacy and New Technology

- **Skype:** Many of the same issues as texting, though Skype is encrypted
  - May want to include on consent forms
  - Not fully compliant with various patient rights

- **Facebook:** How are you using it?
  - Employee training
  - Monitoring
  - Disclaimers

- **Twitter, Snapchat, Periscope, etc.**
Questions?

heyman-layne@alaskalaw.pro

(907) 677-3600
Sedor, Wendlandt, Evans & Filippi, LLC