Privacy, Security and Compliance

February 11, 2017

Alaska Pharmacists Association
Carolyn Heyman-Layne, Esq.

SEDOR WENDLANDT EVANS FILIPPI

1

Learning Objectives

- Recognize the various privacy laws that are applicable to the patient health information pharmacists handle on a daily basis.
- Assess your own privacy programs, policies and procedures generally, to determine if updates or revisions may be necessary to be compliant with the law.
- Review potential violations of HIPAA to determine if outside assistance or other mitigating activities are necessary to address the issue.

2

Covering the Basics

- HIPAA
- Other potential privacy laws: 42 CFR Part 2, Privacy Act, FERPA, AK PIPA, other State laws
- Other healthcare liability concerns
- Effective compliance plans

3

HIPAA Key Concepts: Privacy

- 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.

4

HIPAA Key Concepts: TPO

- Real Life Examples:
  - Sharing PHI with other providers who are also treating the individual.
  - Sharing PHI with an insurance company for payment purposes.
  - Sharing PHI for operations such as peer review or credentialing.
- Remember: Minimum Necessary Only if Not for Treatment!

5

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.

6

HIPAA Key Concepts: Basic Obligations

- 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.

7

Incidental Disclosure (164.502)

- The Privacy Rule permits incidental disclosures to a certain extent – this doesn't mean you can just discuss anything, anywhere!
- Disclosures that occur as a by-product of an otherwise permitted disclosure
  - Disclosure to other patients in a waiting room should be minimized.
  - **Incidental disclosures are permitted only to the extent that the covered entity has applied reasonable and appropriate safeguards and implemented the minimum necessary standard, where appropriate.**

8

Only TWO Mandatory Disclosures

- To the individual
- To DHHS

All others are permissive

Remember: Mandatory vs. permissive
Check for authority

9

HIPAA Security Rule

- 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

10

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

11

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
- Encyrption& Decryption

12

Security Rule: Technical

- Access controls
- Automatic Logoff
- Termination
- Audit Controls
- Integrity
- Person or Entity Authentication
- Data Transmission

13

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!!!

14

HITECH vs. AK PIPA: Breach Reporting

HITECH

- Only covers unsecured protected health information
- Written notification
- More than 500 affected requires notice to media
- Notice within 60 days of discovery
- Specific notice requirements
- Notice to HHS or annual log of breaches

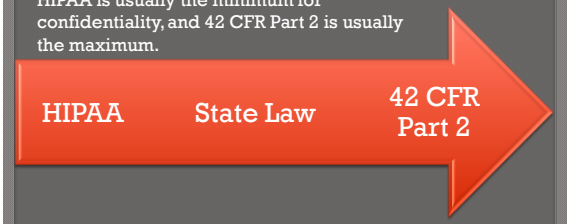
AK PIPA

- Covers "personal information" if reasonable likelihood of harm
- Written or electronic notice
- More than 300,000 requires notice to media
- Requires reporting to AG even if no harm caused
- Make sure this is covered in business associate agreements and vendor contracts

15

HIPAA and 42 CFR Part 2: Degrees of Confidentiality

HIPAA is usually the minimum for confidentiality, and 42 CFR Part 2 is usually the maximum.



Least Strict

Most Strict

16

Other Privacy Laws

- Privacy Act of 1974 – primarily Alaska Native programs, but also Federal agencies
- Alaska Personal Information Protection Act
- FERPA – Family Educational Rights and Privacy Act – schools
- State laws re: substance abuse, behavioral health, etc.

17

Compliance: What, When & Why?

- Affordable Care Act Compliance Requirements
- OIG Guidance
- 7 Elements of an Effective Compliance Plan
- What Should Your Compliance Plan Cover?
- Getting Ready for Enforcement & Audits

18

ACA Compliance Requirements

- Affordable Care Act requires compliance program for providers enrolled in Medicare or Medicaid (including Denali Kidcare)
- HHS and OIG to issue guidance: http://oig.hhs.gov/compliance/101/index.asp
- Timeline still unknown, particularly given new administration
- Auditors may be looking for compliance elements, even if new guidance not issued

19

ACA Compliance Provisions

- Requires Compliance Program as a Condition of Participation in Medicare
  - All providers must certify that they have an effective compliance program
  - Regulations expected for various provider types
  - Enforcement activity increased – MFCU, Audits, etc.
  - Flexibility for varying size providers

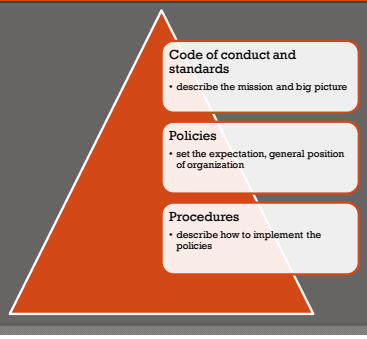
20

Seven Elements of an Effective Compliance Program

- Code of conduct w/written policies & procedures
- Compliance officer, committee and high-level oversight
- Effective training and education
- Effective lines of communication
- Well-publicized disciplinary standards
- Effective system for routine monitoring and auditing
- Prompt response to compliance issues

21

Where to Start?



22

Code of Conduct

- Standards for behavior and actions of everyone in the organization
- Commitment to compliance
- Communicate the Code of Conduct
- Commit resources to the message
- Support the Code of Conduct
- Acknowledge the Code of Conduct

23

Communication

- Communication should go in both directions
- Employees should be provided alternatives for communication
- Hotline process or other anonymous reporting method ideal
- Stress non-retaliation
- Provide variety of forums
- Acknowledge and address employee concerns

24

Monitoring and Auditing

- Regular review of compliance policies and procedures for changes in law, activity, technology, etc.
- Regular review and random audit of records:
  - Documentation of services
  - Billing/Coding
  - Compare to regulations and other written requirements
  - Look for discrepancies
  - Retroactive or concurrent
- Also utilized when suspicions arise, which means baseline is necessary
- Don't forget to audit and monitor training and knowledge of employees
- Feedback to employees after audit

25

Response to Identified Issues

- Mitigation of event/issue
- Evaluation and analysis of event/issue
- Steps to prevent future issues:
  - Disciplinary actions
  - Education and training
  - Changes to policies or procedure
  - New policies and procedures
  - New technologies
  - Reserves for emergency circumstances
- Voluntary Disclosure?
- Outside consultants and/or legal counsel?
- Notification of insurance, other parties?

26

Compliance Checklist

- Develop written compliance program
- Develop employee standards and code of conduct
- Establish and train compliance committee
  - may vary depending on size of organization
- Distribute standards and code of conduct
- Conduct Board/Management training
- Conduct employee training, including info on how to access compliance documents
- Conduct specialized training as necessary
- Establish systems for monitoring

27

On-going Compliance Checklist

- Periodically review compliance program, employee standards and code of conduct
- Ensure that employee training is conducted and documented
- Manage and monitor employee reporting process
- Provide ongoing training, as needed
- Ensure that compliance related files are maintained as described in plan
- Ensure that monitoring and auditing systems are in place and working
- **Make periodic reports to the Board regarding compliance, even if no violations**

28

Laws to Cover in Compliance Program

- Medicare & Medicaid Billing Requirements
- Medicare & Medicaid Documentation Requirements
- Third Party Payor Requirements
- Employment/Labor Law
- Safety Laws
- Reporting Requirements
- HIPAA Privacy & Security
- Stark & Anti-Kickback
- Sarbanes-Oxley
- Licensing Requirements
- Other applicable laws or certification requirements

29

Other areas to review

- Licensing and certification
- Education and training
- Supervision and oversight
- Credentialing and privileges
- Practitioner type
- Location of service
- Scope of practice
- Clinical forms and other paperwork

30

Who enforces healthcare laws?

- State of Alaska, Department of Health and Social Services
- U.S. Department of Health and Human Services
- Office of the Inspector General
- Center for Medicare and Medicaid Services
- FBI
- Department of Justice
- Office of Civil Rights
- State Attorneys General

31

What should you ask?

- What are the risks to the organization?
- What resources are necessary to address those risks?
- Have policies and procedures been implemented to address risks and laws?
- Have training programs been implemented?
- Is the Board informed of changes to regulatory and industry requirements that affect risk?

32

Ok, Who Was Paying Attention?

- Which of the following laws may apply to your pharmacy records?
  1. HIPAA
  2. AK PIPA
  3. 42 CFR Part 2
  4. All of the above
- Under HIPAA, are you required to address both the Privacy and Security Rule in your policies?
- Does the loss of an encrypted laptop require breach reporting?

33

Questions?

heyman-layne@alaskalaw.pro

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

34