Trends in Privacy Policies & Procedures

February 23, 2017
HCCA Alaska Regional Conference
Carolyn Heyman, Esq.

Privacy is not just about HIPAA
Privacy does not exist without security
Security does not work without training, monitoring and auditing
Training is not effective without plain language and examples

Policies and procedures need to include all of the above!
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.

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 PHI.
- Report breaches of PHI.
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

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.
Cover All the Privacy Laws

- Part of your risk assessment should be an analysis of which privacy laws apply
- Policies, procedures and training should cover all applicable privacy laws
- If you work frequently with organizations subject to additional laws (i.e. 42 CFR Part 2 or Privacy Act), may be beneficial to address that possibility

Policy Approach: Privacy Laws

- What do you do when more than one privacy law applies?
  - Look at preemption, provide references, if necessary
  - Cover all applicable laws in one policy, or be sure to reference other policies that may be triggered
  - Examples: HIPAA and AK PIPA; HIPAA and 42 CFR Part 2
Effective Policies Require Effective Training

- Train staff on policies and procedures in using hands-on and interactive methods
- Provide examples, lots and lots of examples
- When new situations arise, send out email alerts
- Make sure employees are familiar with the related forms, not just the policies and procedures

Forms & Templates

- Many policies and procedures may require forms or template documents to be properly and effectively carried out
- Draft the forms before a situation arises
- Make sure forms and templates are patient friendly
- Make sure staff knows when forms should be used
Helpful Privacy Forms

- Forms to exercise privacy rights
- Acknowledgement of staff training
- Acknowledgement of mobile device policies
- Breach notification templates
- Investigation questionnaires

Timeliness is Key!

- Recent action for untimely breach notification resulted in $475,000 payment

"Covered entities need to have a clear policy and procedures in place to respond to the Breach Notification Rule’s timeliness requirements" said OCR Director Jocelyn Samuels.
Many privacy requirements have specific deadlines for follow-up or response
Establish an agreed upon method for tracking deadlines
Include the method in procedures
Be sure that the tracking documents can be accessed by more than just the privacy or security officer

Instead of revising current policies, may be easier to adopt new policies to address:
- HIE Access and Authorization
- HIE Breach Reporting
- HIE Monitoring and Auditing

Look at Network Responsibilities and other contracts, policies for the HIE you are joining
Legal, Technological Changes May Require Policy Changes

- Be sure to monitor laws that affect privacy and security: HIPAA, AK PIPA, new State & Federal laws regarding individual information
- Monitor changes in technology that could affect security:
  - Less expensive alternatives
  - More secure alternatives
  - Changes in staff use of technology

Recent Trends Affecting Privacy

- Storing Data in the Cloud: https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html
- Increased Use of Patient Portals
- Increased Use of Phones and Other Recording Devices
  - Providers
  - Patients
  - Film Crews
Compliance Plans: An Important Part of Privacy

- 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

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
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
On-going Compliance Checklist

- Periodically review compliance program, policies that are part of the 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

Ongoing Compliance Checklist

- 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
Questions?

heyman-layne@alaskalaw.pro

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