Compliance That Addresses the Risks of Today and Will Grow with You in the Future

Objectives

• Identify industry trends and risk for governmental audit/investigation
• Understand the basics of how the seven elements apply to HIPAA compliance
• Become familiar with basic HIPAA rules and tools
• Be able to speak “HIPAA” Privacy and Security
• Know when you need to engage others for help

Still thinking about HIPPOs
Applies to All Organizations

- Don’t have a plan (overwhelmed by HIPAA or still thinking about HIPPOs)
  - Use the 7 elements of an effective compliance plan
  - Supplement with other tools
- You have a plan
  - Make it stronger
  - Areas for improvement
    - risk analysis
    - training

HIPAA is Fun for Everyone

HIPAA Regulations

- Required by LAW
- Penalties for non-compliance
- We see all
HIPAA Regulations

- Privacy/Security is Priority #1
- Breaches
  - Direct to the appropriate staff
  - Candid and Open

HIPAA (applicability)
Covered Entities (CE) and Protected Health Information (PHI)

The Rule (who)
- 45 CFR 160 General Administrative Requirements
- 45 CFR 164 Security and Privacy
- 45 CFR 160.102 and 164.104 – applies to everyone in health care
  - Covered Entity (CE)
    - Health plans
    - Health Clearinghouses
    - Health providers that transmit electronically
  - Business Associates (BA) - certain sections only
Electronic CFR
(code of federal regulations)

§160.103 Applicability.
(a) Except as otherwise provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to the following entities:
(1) A health plan;
(2) A health care clearinghouse;
(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter;
(4) A business associate of a covered entity or any entity that does not fall within paragraphs (1), (2), (3), or (4) of this section.
(b) To the extent required under the Social Security Act, 42 U.S.C. 1320a-7(a)(1), setting in this subchapter shall be reviewed, enforced, and interpreted under the authority of the Inspector General, including such authority as provided in the Inspector General Act of 1978, as amended (5 U.S.C. App.).

Legal Information Institute

§ 160.103 Applicability.
(a) Except as otherwise provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to the following entities:
(1) A health plan;
(2) A health care clearinghouse;
(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter;
(b) To the extent required under the Social Security Act, 42 U.S.C. 1320a-7(a)(1), setting in this subchapter shall be reviewed, enforced, and interpreted under the authority of the Inspector General, including such authority as provided in the Inspector General Act of 1978, as amended (5 U.S.C. App.).

The Rule (what)

• 45 CFR 160.103 Protected health information means individually identifiable health information
• 45 CFR 164 Subpart C—Security Standards for the Protection of Electronic Protected Health Information
Protected Health Information

- Is
  - Transmitted by electronic media;
  - Maintained in electronic media; or
  - Transmitted or maintained in any other form or medium.
- Is not
  - Covered by the Family Educational Rights and Privacy Act (FERPA);
  - "Education Records"
  - Employment records held by a covered entity in its role as employer; and
  - Regarding a person who has been deceased for more than 50 years.

HHS Audits and Investigations

- 200-250 Desk Audits
- Few comprehensive on-site audits (start in 2017)
- Wide range of CEs
- May lead to investigations
Structure

Think of HIPAA Compliance like a house

Not all houses are the same

Basic Structure (7 elements)

- Standards and Procedures
- Oversight
- Education and Training
- Monitoring and Auditing (Risk Assessment)
- Reporting
- Enforcement and Discipline
- Response and Prevention
Basic Materials/Tools
- HHS HIPAA Audit Protocol (in the rules tools)
- 45 CFR 160 and 164
- OIG Guidance
- NIST Standards (National Institute of Standards and Technology)
- Professional Resources
  - HCCA Library
  - HCCA Weekly News
  - Other Professional Organizations (HiMSS, AHIMA, AIHC, etc.)

Start Building

Foundation (Oversight)
- Establish the need
  - Compliance reasons
  - Business Reasons
- Get formal approval from the Governing Board
  - Privacy Officer
  - Security Officer