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)

§160.102 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) Where provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to a business associate.

(c) To the extent required under the Social Security Act, 42 U.S.C. 1320a-7c(a)(5), nothing in this subchapter shall be construed to diminish the authority of any Inspector General, including such authority as provided in the Inspector General Act of 1978, as amended (5 U.S.C. App.).

[65 FR 82798, Dec. 28, 2000, as amended at 67 FR 53266, Aug. 14, 2002; 78 FR 5687, Jan. 25, 2013]

Legal Information Institute

§ 160.102 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) Where provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to a business associate.

(c) To the extent required under the Social Security Act, 42 U.S.C. 1320a-7c(a)(5), nothing in this subchapter shall be construed to diminish the authority of any Inspector General, including such authority as provided in the Inspector General Act of 1978, as amended (5 U.S.C. App.).

[65 FR 82798, Dec. 28, 2000, as amended at 67 FR 53266, Aug. 14, 2002; 78 FR 5687, Jan. 25, 2013]

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

Audit Phase 2

Alert: Phishing Email Disguised as Official OCR Audit Communication - November 28, 2016

It has come to our attention that a phishing email is being circulated on mock HHS Departmental letterhead under the signature of OCR's Director, Jocelyn Samuels. This email appears to be an official government communication, and targets employees of HIPAA covered entities and their business associates. The email prompts recipients to click a link regarding possible inclusion in the HIPAA Privacy, Security, and Breach Rules Audit Program. The link directs individuals to a non-governmental website marketing a firm's cybersecurity services. In no way is this firm associated with the U.S. Department of Health and Human Services or the Office for Civil Rights. We take the unauthorized use of this material by this firm very seriously.

OCR would like to further share that this phishing email originates from the email address OSOCRAudit@hhs-gov.us and directs individuals to a URL at http://www.hhs-gov.us. This is a subtle difference from the official email address for our HIPAA audit program, OSOCRAudit@hhs.gov, but such subtlety is typical in phishing scams.

Covered entities and business associates should alert their employees of this issue and take note that official communications regarding the HIPAA audit program are sent to selected auditees from the email address OSOCRAudit@hhs.gov. In the event that you or your organization has a question as to whether it has received an official communication from our agency regarding a HIPAA audit, please contact us via email at OSOCRAudit@hhs.gov

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