







Elements of HIPAA

- Privacy Standards (4/14/03)
- Transactions and Code Sets (10/16/03)
- National Employer Identifier (7/30/04; 8/1/05)
- Security Standards (4/21/05; 06)
- Enforcement Rule (3/16/06)
- National Provider Identifier (5/23/07; 08)
- Breach Notification (9/23/09)

ARRA 2009

- HITECH Act of the American Recovery and Reinvestment Act of 2009 (ARRA) imposes new obligations on covered entities (CE) and business associates (BA).
 - Breach Notification
 - BA directly responsible for compliance with the Security Rule and directly liable for violations of the Security Rule and breaches.

Who Does HIPAA affect?

EVERYONE!

Definitions

- Protected Health Information (PHI) & e-PHI
- Covered Entity (CE)
- Business Associate (BA)
- Use
- Disclosure
- Minimum Necessary
- Improper use/disclosure
- Security Incident
- Breach

Protected Health Information (PHI)

- “individually identifiable health information...that is:
 - Transmitted by electronic media;
 - Maintained in electronic media; or
 - Transmitted or maintained in any other form or medium.”
- 45 CFR sec. 160.103

E-PHI

- PHI that is transmitted and/or maintained in an electronic format.
- 45 CFR sec. 160.103

Covered Entity (CE)

- A CE must comply with HIPAA.
- A CE is:
 - A health plan;
 - A health care clearinghouse; or
 - A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.
 - 45 CFR sec. 160.103

Business Associate (BA)

- A person/company/firm that performs a function for the CE that requires the use, disclosure, or creation of PHI.
- A BA may also be a CE.
 - 45 CFR sec. 160.103

Use

- "Use" means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information."
 - 45 CFR sec. 160.103

Disclosure

- “Disclosure means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.”
 - 45 CFR 160.103



Minimum Necessary

- “When using or disclosing PHI or when requesting PHI from another CE, a CE must make reasonable efforts to limit PHI to the **minimum necessary** to accomplish the intended purpose of the use, disclosure, or request.”
 - 45 CFR sec. 164.502(b)(1)

Improper Use or Disclosure

- BAs must report to DSS:
 - Uses or disclosures not permitted or required by the Business Associate provisions of their respective contract(s) or by HIPAA.

Security Incident

- BAs must report to DSS:
 - Attempted or successful unauthorized access, use, modification, or destruction of information or interference with systems operations in an information system.
 - 45 CFR 164.304

Breach

- Unauthorized acquisition, access, use, or disclosure of PHI which compromises security or privacy of information, except where the unauthorized person to whom such information is disclosed would not reasonably have been able to retain the information.
- 42 USC sec. 17921 & 45 CFR sec. 164.402

Breach Notification

- Notice sent to an individual of a breach of his/her PHI is required under the ARRA HITECH Act!
- Breaches involving PHI of more than 500 individuals in one incident must be immediately reported to HHS by the CE for posting on the HHS website.
