HIPAA Compliance

Presented By | Adam Jensen, Vice President

Cottingham & Butler

PRESENTER

ADAM P. JENSEN

JD, MS-HRM, CEBS, GBA, FLMI

Vice President, Compliance & HR Consulting

ajensen@cottinghambutler.com

608.467.5030

A BRIEF HISTORY

The Health Insurance Portability & Accountability Act of 1996 includes several Titles.

- Title I – PORTABILITY of coverage.
- Title II – ADMINISTRATIVE SIMPLIFICATION, INCLUDING THE PRIVACY AND SECURITY RULES.
  - This presentation focuses on this area.

HIPAA'S STRUCTURE

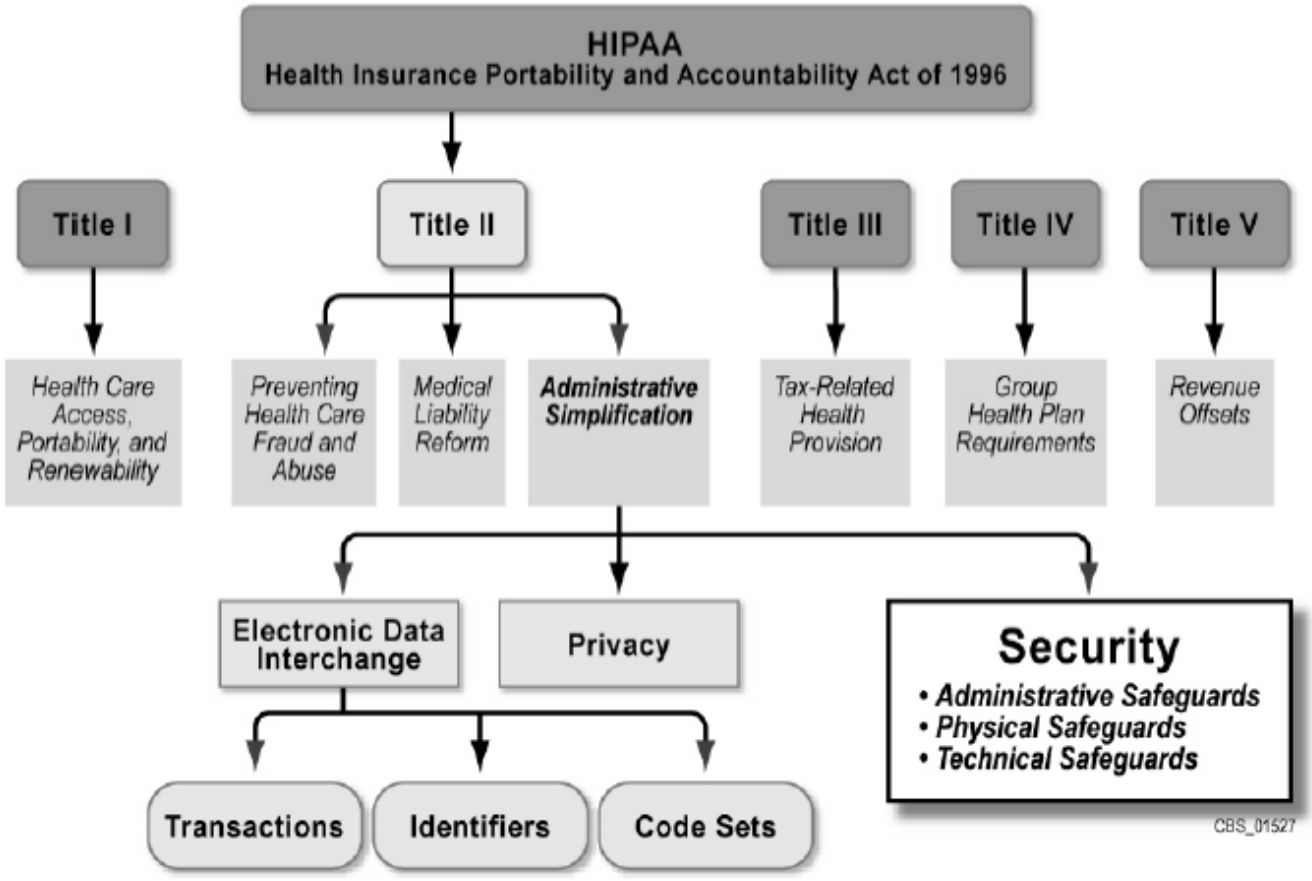

Figure 1. HIPAA Components

HIPAA'S PRIVACY AND SECURITY RULES

HIPAA Title II –

- "ADMINISTRATIVE SIMPLIFICATION"
  - Privacy Rule
  - Security Rule

HIPAA'S PRIVACY AND SECURITY RULES

HIPAA Privacy Rule

- Applies to all Protected Health Information created or maintained by the plan.

HIPAA Security Rule

- Similar to the Privacy Rule, but specifically deals with Electronic Protected Health Information.

HIPAA GENERAL RULE

General Rule:

"A Covered Entity may not use or disclose protected health information, except as otherwise permitted or required."

WHAT IS A COVERED ENTITY?

- Health Plans (ERISA plans, HMOs, licensed insurers, Medicare, etc.).
- Providers who conduct one or more of the HIPAA-defined transactions electronically (physicians, hospitals, pharmacies, chiropractors, dentists, etc.).

WHAT ARE COVERED ENTITY OBLIGATIONS UNDER HIPAA?

The Covered Entity must:

- Take reasonable and appropriate precautions against reasonably anticipated risks to protect individually identifiable information created or maintained by the health plan.
- Must comply with both the Privacy and Security Rules!
  - Applies to medical, dental, vision, and Rx plans.

WHAT ARE COVERED ENTITY OBLIGATIONS UNDER HIPAA?

Programs/Benefits Excluded from HIPAA:

- Workers' Compensation
- Family Medical Leave Act
- Short-Term/Long-Term Disability
- Life Insurance

WHAT IS PROTECTED HEALTH INFORMATION (PHI)?

- Health and demographic information about an individual that is transmitted or maintained in any medium where the information:
  - is created or received by a health care provider, health plan, or health care clearinghouse; and
  - relates to the past, present, or future:
    - physical or mental health condition of an individual, or
    - provision of health care to an individual, or
    - payment for the provision of health care to an individual.

WHAT IS PROTECTED HEALTH INFORMATION (PHI)?

PHI is health information that is individually identifiable. Individual identifiers can include:

- Name
- All geographic information (state, street address, city, zip code, etc.)
- Dates (birth dates, admission dates, date of hire, etc.)
- Telephone and fax numbers
- Email addresses
- Social Security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Certificate or license numbers
- Vehicle identifiers and serial numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Biometric identifiers, such as fingerprints or voice prints
- Full face photographic images
- Any other unique identifying number, characteristic or code

WHAT IS EPHI?

EPHI is individually identifiable health information that is:

- Transmitted by electronic media;
- Maintained in electronic media; or
- Transmitted or maintained in any other form or medium.

WHAT QUALIFIES AS ELECTRONIC MEDIA?

Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium such as magnetic tape or disk, optical disk, or digital memory card; or

Transmission media used to exchange information already in electronic storage media. Transmission media includes:

- Internet, extranet, leased lines and dial-up lines; private networks; and
- the physical movement of removable/transportable electronic storage media.

SPECIAL NOTES ON ELECTRONIC MEDIA

No distinction is made between data movement – internal or external to the organization, nor between data “at rest” (stored) or in transit over wire, fiber or other media.

The standard applies equally to all.

SPECIAL NOTES ON ELECTRONIC MEDIA

Certain transmissions, including of paper, via fax, and of voice, via telephone are not considered to be transmissions via electronic media, because the information being exchanged did not exist in the electronic form before the transmission.

Understand however, that the Privacy Rule is normally interpreted as requiring appropriate security measures for PHI of all kinds and would include all of these.

INFORMATION SYSTEMS

The Security Rule reaches to electronic “systems” which is defined as:

- An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.
  - To be effective, Security must be applied to the entire system. Hence the completeness of the Rules – Administrative, Physical and Technical “**Safeguards**” requirements.

USE OF PHI

Under the Privacy Rules, “USE” means (with respect to individually identifiable health information) the:

- sharing,
- employment,
- application,
- utilization,
- examination, or
- analysis

of such information within the covered entity is holding the information.

DISCLOSURE OF PHI

Under the Privacy Rules, “Disclosure” means the:

- Release,
- Transfer,
- Provision of access to, or
- Divulging in any other manner

of information outside the covered entity holding the information.

PERMITTED USES AND DISCLOSURES

Covered Entities is permitted to use and disclose PHI for:

- Treatment
- Payment
- Health Care Operations

These are known as “TPO”.

PERMITTED USES AND DISCLOSURES

A Covered Entity may:

- Use or disclose PHI for its own TPO.
- Disclose PHI to another entity for TPO activities.

Most other uses or disclosures that are not TPO require an Authorization from the individual to whom the PHI is related.

TPO – HEALTH CARE OPERATIONS

Health Care Operations of a Covered Entity include:

- Underwriting, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance
- Business planning and development
- Business management and general administrative activities
- Medical review, legal services, and auditing
- Quality assessment and improvement and population-based activities
- Peer review and credentialing activities

AUTHORIZATIONS

Authorizations must be obtained from the individual whose PHI is being used or disclosed for purposes outside of TPO or those mandated under law.

- Some of the information an Authorization must include is (Covered Entities has a standard authorization form to be used):
  - A description of the information to be disclosed;
  - The name of the person or entities to whom the information will be disclosed;
  - The date upon which the authorization will expire;
  - A statement that the individual can revoke the authorization at any time; and
  - Date and signature.

UNAUTHORIZED USES DISCLOSURES

An unauthorized use or disclosure of PHI that could reasonably result in significant harm to an Individual is a “breach”.

- Possible breaches must be reported to the Privacy Officer.
- Privacy Officer will review and if necessary report to the individual(s) whose PHI was breached and the U.S. Dept. of Health and Human Services within 60 days of discovering the breach.
- If over 500 persons affected by breach, news media may have to be notified.

MINIMUM NECESSARY STANDARD

The Privacy Rules require Covered Entities to make reasonable efforts to limit use, disclosure of, and requests for PHI to the minimum necessary to accomplish the intended purpose.

Covered Entities must make their own assessment of what PHI is reasonably necessary for a particular purpose, given the characteristics of their business and workforce, and to implement policies and procedures accordingly.

MINIMUM NECESSARY STANDARD

A reasonableness standard should be used consistent with the best practices and guidelines to limit the unnecessary sharing of medical information.

You do need to limit information uses or disclosures to those that are absolutely needed to serve the purpose.

MINIMUM NECESSARY STANDARD

Is intended to:

- Make you evaluate your practices and enhance protections as needed to prevent unnecessary or inappropriate access to PHI; and

- Reflect and be consistent with (not override) professional judgment and standards.

MINIMUM NECESSARY STANDARD

The Privacy Rules identify three categories of uses and disclosures, and impose different compliance requirements for the minimum necessary standard in each category.

The three categories are:

- Internal use of PHI
- Routine disclosures of PHI
- Non-routine disclosures of PHI

MINIMUM NECESSARY STANDARD

Internal use of PHI

- Covered Entities must:
  - Identify the individuals or classes of persons who require access to plan member PHI to carry out their respective job duties.
  - Identify the categories or types of PHI that each of these individuals or classes of persons require.
  - Identify under what conditions such individuals or classes of persons will require access to PHI to perform their respective job duties.
- Policies and procedures must be implemented to ensure that the use of PHI remains limited to the amount that is the minimum necessary for the intended purpose.

MINIMUM NECESSARY STANDARD

Routine Disclosures:

- Covered Entities must develop standard policies and procedures for routine or recurring disclosures to entities outside the health plan.
- The policies and procedures should limit the PHI disclosed to the minimum necessary to achieve the purpose of that particular disclosure.

MINIMUM NECESSARY STANDARD

Non-routine disclosures:

- Covered Entities must implement policies and procedures to determine the minimum amount of PHI necessary to accomplish each intended purpose of the non-routine disclosure.
- Each non-routine request must be reviewed on a case-by-case basis to ensure only the minimum amount necessary of PHI is disclosed.

ADMINISTRATIVE REQUIREMENTS

Covered Entities Must:

- Designate a Privacy Officer, Security Officer, and Contact Person
- The Privacy Officer is in charge of creating and implementing the policies and procedures to bring a health plan into compliance with the Privacy Rules.
- Security Officer is like the Privacy Officer, but deals with EPHI.
- The Contact Person(s) is responsible for the day-to-day operations of the health plan's privacy policies and procedures.

ADMINISTRATIVE REQUIREMENTS

Covered Entities must document policies and procedures regarding the handling of PHI.

ADMINISTRATIVE REQUIREMENTS

Covered Entities Must:

- Provide training to their “workforce” regarding the policies and procedures implemented to protect PHI.
- “Workforce” is defined as being: employees, volunteers, and other persons whose conduct, in the performance of work for a covered entity, is under the entity’s direct control, whether or not they are paid by the covered entity.

ADMINISTRATIVE REQUIREMENTS

A system of safeguards to protect PHI should be created.

- These safeguards should include:
  - Documents containing plan member PHI (i.e., renewal reports, copies of EOB's etc.) should be shredded when no longer necessary and prior to disposal;
  - Requiring that doors to areas containing plan member PHI (or file cabinets housing such records) remain locked and limiting which personnel are authorized to have the key or password.
  - Discussions with plan participants should be conducted in a place and manner in which overhearing the discussion by others will not occur.
  - Email transmissions of plan member PHI should be confidential.
  - Ensure that plan member protected health information is not visible at locations not under secured settings.
  - All systems that house plan member PHI will have access limited through the use of passwords that will change periodically. All passwords should be safeguarded.
  - PHI that is located on computers soon to be discarded should have hard drives cleared of all data.
  - Any plan member PHI that is lost or missing from respective areas be reported immediately to the Privacy Officer for proper mitigation efforts.
  - Any plan member PHI held by a terminated Business Associate, should be requested to be returned to Covered Entities if feasible.

ADMINISTRATIVE REQUIREMENTS

Covered Entities cannot require individuals to waive their rights as a condition of payment, enrollment or eligibility for benefits.

Covered Entities must have complete and accurate documentation of all compliance activity.

Business Associate Agreements must be entered into.

BUSINESS ASSOCIATES

A business associate is a person or entity who either provides services on behalf of Covered Entities, or to Covered Entities which involves the use or disclosure of PHI.

A business associate is not a member of the Covered Entities' workforce.

Covered Entities may only disclose PHI to business associates if satisfactory assurances are received that the business associate will safeguard the PHI.

INDIVIDUAL RIGHTS UNDER THE PRIVACY RULES

Right to receive written notice of privacy practices.

- A written notice must be distributed.
- All new hires must receive a copy of the notice.
  - Fully-insured plans will have notices issued by the insurance carrier.

INDIVIDUAL RIGHTS UNDER THE PRIVACY RULES

- Request restrictions on uses and disclosures.
- Inspect and copy one's own PHI.
- Request to receive PHI by alternative means or at an alternate address.
- Request amendment or correction of their PHI.
- Receive an accounting of disclosures of their PHI (except those related to TPO).

ENFORCEMENT

- The U.S. Dept. of Health and Human Services, Office For Civil Rights (OCR) enforces compliance.
- Covered Entities is subject to audits by HHS/OCR.

POTENTIAL PENALTIES FOR NON-COMPLIANCE

Criminal Penalties

- Up to $50,000 and up to one year in prison for inappropriately using or disclosing PHI.
- Up to $100,000 and up to five years in prison for using or disclosing PHI under false pretenses.
- Up to $250,000 and up to ten years in prison for using or disclosing PHI with the intent to sell, transfer, or use it for commercial advantage, personal gain or malicious harm.

POTENTIAL PENALTIES FOR NON-COMPLIANCE

Civil penalties for non-compliance

- $100/violation not to exceed $50,000/calendar year
  - if did not know of violation and would not have known even with reasonable diligence.
- $1,000/violation not to exceed $50,000/calendar year
  - if due to reasonable cause and not willful neglect.
- $10,000/violation not to exceed $50,000/calendar year.
  - penalty if willful neglect but corrected within 30 days.
- At least $50,000/violation not to exceed $1,500,000/calendar year
  - penalty if willful neglect, but not corrected within 30 days.

THANK YOU FOR VIEWING!

ADAM P. JENSEN

JD, MS-HRM, CEBS, GBA, FLMI

Vice President, Compliance & HR Consulting

ajensen@cottinghambutler.com

608.467.5030