The Health Insurance Portability and Accountability Act (HIPAA): The Basics

Presented by:

www.TheHealthLawFirm.com

THE HEALTH LAW FIRM

George F. Indest III, J.D., M.P.A., LL.M.
Board Certified by the Florida Bar in the Legal Specialty of Health Law

Website: www.TheHealthLawFirm.com

THE HEALTH LAW FIRM

Main Office:
1101 Douglas Avenue
Altamonte Springs, Florida 32714

Phone: (407) 331-6620
Fax: (407) 331-3030

Website: www.TheHealthLawFirm.com

Useful Websites

- http://aspe.hhs.gov/admnsimp/Index.htm
- http://www.cpri-host.org/resource/toolkit/toolkit.html
- http://dirm.state.nc.us/hipaa/hipaa2002/privacy/privacy.html

HIPAA BASICS

HIPAA Administrative Simplification Provisions

- Provide requirements for the electronic transmission of health care information
  - Electronic signatures
  - Unique identifiers
  - Standards for designated transactions
  - Security and privacy standards

Privacy Protections

- Final Rule Published – 12/28/00
- Final Modifications Published – 8/14/02
- Compliance Date – 4/14/02
- More Stringent State Laws

The Basics of the "Final" HIPAA Privacy Regulations

- Basic Purpose: To ensure the privacy of health information that is maintained or transmitted.

- Basic Rule: Covered entities may not disclose individually identifiable health information unless authorized

Scope of the Regulations

- Are you a covered entity?
- Is the information protected?

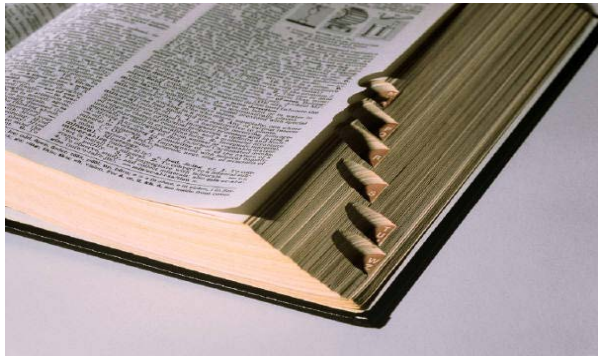
  Note - the entire medical record is not protected.
- If yes to both, is the disclosure authorized?

Key Definitions

Covered Entity

Health Care Operations

PHI



What is a Covered Entity?

- Only certain types of entities are covered
  - Health Plans
  - Health Care Clearinghouses
  - Health Care Providers that transmit health information in electronic form in connection with standard transactions.

What is a Health Care Provider?

- Hospital
- SNF
- Home Health Agency
- CORF
- Clinic
- Lab
- Group Practices
- Pharmacies
- ASCs
- Licensed Practitioners
  - **MDs**
  - **Nurses**
  - **ARNPs**
  - **PAs**
  - **Therapists**
  - **DCs**

What is a Health Plan?

- Group health plan
- Health insurance issuer
- Medicare/M+C
- Medicaid
- Issuer of Medicare supplemental policies
- FEHB
- State high risk pools
- Issuer of long-term care policies
- Health care program:
  - military personnel
  - Veterans
- CHAMPUS
- Indian Health Service
- Other plans that pay or provide medical care

Hybrid Entities

- Covered entity components of non-covered entities must comply with the regulations.
- If CE qualifies as an HE, it can elect its status.
- If the CE chooses to be an HE, it must designate its health care components & establish safeguards
- Examples:
  - Employee or school health clinic
  - Self-funded insurance plans
  - Researchers who provide health care to subjects
  - Government agency covered plans or providers

CEs with Multiple Covered Functions

- Must comply with standards, requirements and implementation specifications, as applicable to the covered functions performed.
- Use or disclosure of PHI is limited to purposes of function being performed.
- Example – CE which operates a Health Plan and Health Clinics

Health Care Operations

- QA & PI activities;
- Evaluation, training, accreditation, certification, licensing or credentialing providers;
- Conducting medical review, legal services, audits & compliance programs;
- Business planning & development; and
- Management/administration activities

PHI

- Individually identifiable;
- Related to a condition, provision of care, or payment;
- Created or received by a covered entity; and
- Transmitted or maintained by electronic media or in any other form.

What is Individually Identifiable Health Information?

- Name
- Address
- Employer
- Relative's Name
- DOB
- Telephone & Fax #
- e-mail Address
- IP Address
- SSN
- MRN
- Member or Account #
- Driver's License #
- Voice/fingerprints
- Photos

Employment records are not PHI when held by CE in its Employer role

Transmission/Maintenance

- Electronic Media - is the source or target of the information exchange a computer? Examples: floppy disk, Internet, dial-up lines, leased lines, and private networks

- Any Other Form or Medium - expands the definition to include paper records and, arguably, oral health information.

General Rules for Use and Disclosure of PHI

General Rule

Minimum Necessary Requirement

Verification Requirement

4 Types of Uses and Disclosures

- Treatment, Payment, Health Care Operations
- Opportunity to Agree/Object Required
- Nothing Additional Required
- Authorization Required

General Rule

Covered entities are prohibited from using or disclosing protected health information without consent.

Minimum Necessary Rule

- Covered entities must make reasonable efforts to limit use, disclosure or requests of PHI to the minimum necessary to accomplish the intended purpose.
- Exceptions:
  - For treatment;
  - To or by the individual;
  - Made pursuant to an authorization;
  - To HHS for compliance investigations; and
  - Required by law.

Incidental Uses/Disclosures

- Definition:
  - Secondary U/D that can't be reasonably prevented;
  - Limited in nature; and
  - Occurs as by-product of permitted U/D
- To qualify – implement reasonable safeguards & the minimum necessary standard
- N/A to errors, mistakes, neglect

Verification Requirement

- Verify the identity and authority of a person requesting PHI.

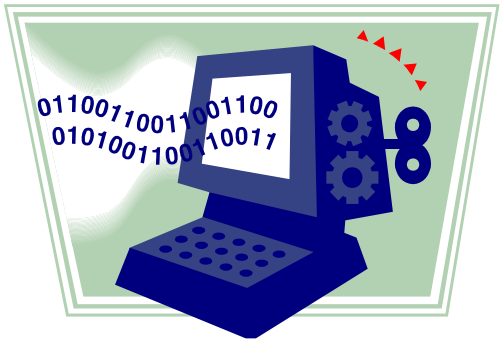
- Obtain any documentation, statements, or representations from the person requesting PHI when required by HIPAA.

De-identification of PHI

Purpose & Rule

Methods

Limited Date Sets



Purpose & Rule

- Once PHI is de-identified, HIPAA does not apply.
- A covered entity may use or disclose PHI to de-identify the information.
- Once the information is re-identified, HIPAA applies, so safeguards must be in place.

Methods for De-Identification

- Expert Determination
- Removal of Identifiers:
  - Names
  - Geography
  - Dates
  - Phone/SSN/MRN/Account Numbers
  - e-mail addresses, etc.
  - Photos/fingerprints/voice prints

Limited Data Sets

- Remove:
  - Names
  - Street Address/Phone & Fax Numbers/e-mail
  - SSN/License #/VIN/Serial #/Account #
  - Full face photos/biometric identifiers
- Purposes: research, public health, HCO
- Requirements: obtain data use agreement from recipient

Use/Disclosure to Carry Out Treatment, Payment or Health Care Operations

Permitted Uses and Disclosures

Psychotherapy Notes

Permitted Uses & Disclosures

- Treatment: CE may U/D for treatment activities of the CE or another healthcare provider
- Payment: CE may U/D for payment activities of CE or another CE or health care provider
- HCO: CE may U/D for its own HCO or limited HCO of another CE (if relationship with individual):
  - QA/case management
  - Conducting training, accreditation, licensing, credentialing

Psychotherapy Notes

- May not use or disclose PHI for TPO, except:
  - Use by the originator for treatment;
  - CE's own training purposes; and
  - By CE to defend itself in legal action brought by individual.
- May/must disclose for purposes of oversight, compliance with laws, death identification and prevention of threats

When is an Authorization Required?

General Rule

Requirements

Additional Notes

General Rule

A covered entity may not use or disclose PHI without a valid authorization, unless permitted by HIPAA. Use or disclosure of PHI must be consistent with the authorization.

CE must have an authorization to U/D psychotherapy notes with limited exceptions.

Marketing

- CE must obtain authorization prior to use/disclosure for marketing communications, unless:
  - Face to face communication
  - Involves gift of nominal value
- Must include statement about remuneration
- 456.057(5)(b) – Requires auth for use of patient info to solicit/market sale of goods & services

Core Requirements

- Description of the information to be used or disclosed;
- Identification of the person(s) authorized to make/receive the requested use or disclosure;
- Description of each purpose of the use/disclosure;
- Expiration date or event;
- Plain language, signed and dated;

Core Requirements Cont'd

- Statement of revocation right;
- Statement that PHI may be redisclosed; and
- Statement that conditioning is prohibited (w/ ltd exceptions); and
- If the CE sought the authorization, a statement that the individual may obtain a copy of the signed authorization.

Prohibition on Compounding

- May not combine auth with other documents
- Psychotherapy notes – may only combine with another auth for U/D of psychotherapy notes
- Other authorizations may be combined unless one of the authorizations contains conditions

Additional Notes

- A covered entity may not condition treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization with limited exceptions.
- Authorizations may be revoked at any time.
  - Must be in writing.
  - Not effective if CE relied & acted on authorization.
- A covered entity must document and retain any signed authorization.

Additional Notes

- Minimum necessary standard does not apply to disclosures made pursuant to an authorization.
- Disclosures pursuant to an authorization are not subject to accounting requirements

When Must You Provide an Opportunity to Agree or Object?

General Rules

Facility Directories

Involvement in the Patient's Care and Notification Purposes

General Rule

- Covered Entity must inform the patient and provide an opportunity to restrict or limit use or disclosure.
- Emergency - may use/disclose if in individual's best interests and consistent with prior preferences. Must inform and provide opportunity to object when able.

Facility Directories

- May disclose to:
  - Members of the clergy; or
  - Those who ask for the individual by name (except for religious affiliation)

Involvement in Care and Notification Purposes

- May disclose to:
  - To a family member, etc., involved with the individual's care or payment for care.
  - To notify, or assist in the notification of a family member, etc., of the individual's location, general condition, or death.

When is Consent, Authorization or Opportunity to Agree/Object Not Required?

12 Uses and Disclosures

Nothing Required

- Required by law;
- Public health activities;
- Reports of abuse, neglect;
- Health oversight activities;
- Judicial proceedings;
- Law enforcement;
- Coroners;
- Research purposes;
- Organ donation;
- Prevent threats to health and safety ;
- Specialized government functions;
- Workers' comp.

Applicable to all Covered Entities

Individual Rights under HIPAA

- Right to notice
- Right to request privacy protection for PHI
- Right to access, inspect & copy PHI
- Right to request amendment
- Right to receive an accounting
- Right to file complaint with any covered entity or with HHS.

Privacy Practices

- All CEs must provide NPP.
- Exception for Inmates
- Lengthy Exception for Group Health Plans
- Up to 21 Core Elements
- Specific time provisions for health plans and providers with direct treatment relationships
- If CE has a web site with service/benefit info, NPP must be posted.

Provision of Notice

- Direct Treatment Providers:
  - At time of 1st treatment encounter
  - Must make a good faith effort to obtain acknowledgement of receipt
- Other CEs:
  - Make it available on request

Privacy Protection

- Right to request restrictions
  - CE not required to honor
- Confidential communications
  - CE may require written request, provision of alternative means of contact, info on how payment will be made (if applicable)
  - Providers must accommodate reasonable requests
  - Health plans must accommodate reasonable requests, if individual clearly states disclosure could endanger

Accounting

- Right to receive accounting of disclosures of PHI within past 6 years
- Exceptions:
  - TPO
  - To individual/ pursuant to authorization
  - LDS
  - For national security
  - To correctional institutions
  - Occurred prior to compliance date (sort of)

Actual Chart Entries

- Discharge status: Alive but without permission.
- By the time he was admitted, his rapid heart had stopped, and he was feeling better.
- Patient has left his white blood cells at another hospital.

New Obligations under HIPAA

- Notice of information practices
- Designate a privacy official
- Designate compliance contact
- Provide training
- Implement safeguards
- Complaint process
- Sanctions
- Duty to mitigate
- No retaliation
- Can’t condition services on complaint waiver
- P & P on PHI
- Documentation (6 years)
- Additional requirements for group health plans

Business Associates

Definition

Disclosure to Business Associates

Contract Requirements

Definition

- A person to whom a covered entity discloses PHI so that the person can perform a function or activity for the covered entity.
- Examples:

  Lawyers, Auditors, TPAs, Consultants, Data processing firms, Billing firms, Other covered entities

Business Partners Do Not Include:

- Employees, volunteers
- Those with whom the covered entity does not share PHI
- Those who do not provide services to the covered entity

Disclosure Standard

- Covered entities may disclose PHI & allow business associates to create or receive PHI, if the covered entity obtains satisfactory assurances of safeguards.
- The standard does not apply to disclosures for treatment purposes (i.e. consults).
- Contract must be in place before PHI shared

Contract Requirements

- Must establish permitted uses & disclosures
- Must prohibit use/disclosure:
  - other than for purpose stated in contract or
  - that would violate the regulations.

Contract Requirements

- Must require:
  - Safeguards (and document assurances)
  - Report of any wrongful use/disclosure
  - Return/destruction of PHI when contract terminates
- Must allow for termination by covered entity if the business associate violates a material term of the contract.

Transition Provisions

- One Year Extension
  - Contracts entered into prior to 10/15/02
  - Only if contracts not modified prior to the effective date
  - Extension does not apply to oral contracts
- Ensure cooperation of BAs in fulfilling individual rights
- Sample Language Language

Confidentiality Agreement

- Not required by HIPAA but good business practice
- Use:
  - Employees
  - Contractors that are not Business Associates
- Elements:
  - Agree to protect privacy
  - Indemnification

Application of Other Laws under HIPAA

- General Rule: Contrary state laws would be preempted.
- Exceptions:
  - Laws Exempted by HHS
  - More stringent state law
  - Public health laws
  - Licensure/certification laws
- FHA has a Preemption Analysis available

Enforcement

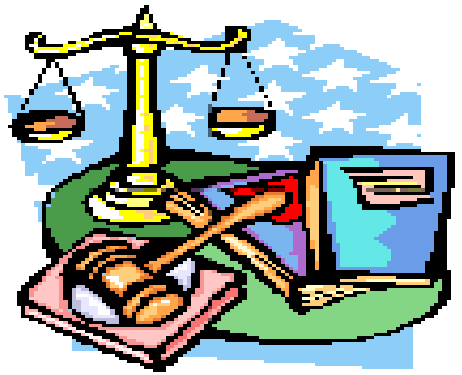
- Civil Monetary Penalties
  - $100 cap per violation
  - $25,000 cap per person per year for violations of a single standard
- Criminal Offense
  - Up to $250,000 fine and/or 10 years in prison
- Threat of civil litigation

Cost of Compliance

- HHS estimate: $17.6 billion over ten years
- BC/BS estimate: $43 billion
- Tillinghast-Towers Perrin estimates:
  - $775,000 - $3.5 million for mid-size hospitals
  - $75,000 to $250,000 for 50-member physician groups

DORLAND'S ILLUSTRATED MEDICAL DICTIONARY

Lawyer - n. Professionals who get us out of all the trouble we would never have been in if it hadn't been for the lawyers.



The Health Law Firm

Main Office:
1101 Douglas Avenue
Altamonte Springs, FL 32714

Phone: (407) 331-6620
Fax: (407) 331-3030

Website: www.TheHealthLawFirm.com

THE HEALTH LAW FIRM

Orlando Office (By Appointment):

37 North Orange Avenue, Suite 500
Orlando, Florida 32801

Phone: (407) 331-6620
Fax: (407) 331-3030

Website: www.TheHealthLawFirm.com

THE HEALTH LAW FIRM

Pensacola Office (By Appointment):

201 East Government Street
Pensacola, Florida 32502

Phone: (850) 439-1001
Fax: (407) 331-3030

Website: www.TheHealthLawFirm.com

THE HEALTH LAW FIRM

Denver, Colorado Office (By Appointment):

155 East Boardwalk Drive, Suite 424
Fort Collins, Colorado 80525

Phone: (970) 416-7454
Fax: (866) 203-1464

Website: www.TheHealthLawFirm.com