HIPAA OVERVIEW

The Health Insurance Portability and Accountability Act of 1996

Philip M. Bluestein, Esq
5600 Arapahoe Ave.
Suite 201
Boulder, Colorado 80303
(303) 880-4998
pmblue@bluesteinlaw.com
www.bluesteinlaw.com

What is HIPAA?

- It's HIPAA Not HIPPA or HIPPO

What is HIPAA?

- **H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct of 1996
- Pub.L. No. 104-191, 110 Stat. 1936 (1996)
- 42 USCS § 1320d-2
- Regulations Contained at 45 CFR Part 164 Security and Privacy

What Does HIPAA Do?

- HIPAA provides a comprehensive and uniform standard for healthcare providers for the use and disclosure of confidential patient information.
- Creates a floor of protection and establishes some level of uniformity.
- Generally, HIPAA does not pre-empt state laws
  - Will preempt state laws which are less stringent than HIPAA
- Allows Patients access to their own information

Who is Covered by HIPAA?

- Covered Entities – Who is a covered entity?
  - Health Care providers who transmit information electronically (basically everyone)
  - Health Plans – includes group health plans including 50 or more employees, lots of others
    - (Workers Compensation not covered)
  - Clearing Houses – Entities doing billing and collection that submit bills on behalf of health care providers

Protected Health Information

What Information Does HIPAA Apply to?

- Protected Health Information (PHI)
  - PHI includes individually identifiable health information that is transmitted electronically, maintained electronically, or transmitted or maintained in any other form or medium.
  - PHI includes oral information and written records
  - Does not include De-Identified Information

Disclosures of PHI

- Different Types of Disclosures
  - Disclosures Permitted with Authorization
  - Disclosures Permitted without Authorization
  - Disclosure Exceptions
  - Impermissible Disclosures

Disclosures of PHI

- Disclosures with Patient Authorization
  - Generally Covered Entities may not disclose PHI without the authorization of the Patient.
  - Specific contents of the authorization are outlined in the statute
  - A Covered Entity may not condition the provision of treatment, payment, enrollment in the health plan or eligibility for benefits on an individual executing an authorization

Disclosures of PHI Continued

- Disclosures without Authorization
  - Covered Entities may disclose PHI without Authorization for purposes of:
    - Treatment – May disclose information for the purposes of treatment of the individual and may disclose it to other providers for the purposes of treatment
    - Payment – May disclose to another entity for payment purposes
    - Healthcare Operations – May disclose to certain other entities that have a relationship with the individual

Disclosures of PHI Continued

- Exceptions
  - Disclosure required by law
  - Victims of domestic abuse or violence
  - Judicial or administrative proceedings
  - Imminent threats to health or safety
  - Specialized rules and functions

Disclosures of PHI Continued

- De-Identified Information
- Information that is "De-Identified" can be disclosed by covered entities
  - De-Identified Information is information that has had specific information removed such as names, addresses, social security numbers, account numbers, medical record numbers, phone numbers or other unique identifying characteristic, code or information that would allow someone to determine who the information relates to
- Examples of Uses of De-Identified Information:
  - Statistics
  - Studies

Disclosures of PHI Continued

- Generally all other Disclosures of PHI by a Covered Entity are violations of HIPAA

Disclosures – Business Associates

- Business Associate Agreements
  - Covered Entities must enter into contracts with their business associates requiring the business associate to maintain the confidentiality and security of the PHI

Disclosures – Minimum Necessary

- Except for certain exceptions – every disclosure must comply with "minimum necessary".
- The Covered Entity must only disclose the minimum amount of information necessary for the recipient on the other side.
- Minimum Necessary does not apply to
  - Disclosures for the purposes of Treatment
  - Disclosures to the Individual (patient requests)
  - Disclosures with Written Authorization
  - Disclosures Required by law

What Do My Clients Need to Do

- Notice of Privacy Practices
- Security
- Training
- Privacy and Security Officer
  - Not just a title

Notice of Privacy Practices

- Notice of Privacy Practices sets forth the permitted uses and disclosures of the individual's PHI, the Covered Entities obligations and the individuals rights regarding their PHI
- Certain mandatory information that must be included in the Notice

Security

- Covered Entities must
- Ensure the confidentiality, integrity and availability of all electronic protected health information the covered entity creates, receives, maintains or transmits.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of e-PHI.
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required
- Ensure compliance with the Security Rule by the covered entity's workforce.

Training

- A Covered Entity must train all of its workforce on the privacy policies and procedures with respect to PHI to carry out their duties
- Training should be provided for new employees
- Training of employees should be documented

Privacy and Security Officer

- A Covered Entity must designate a privacy and security officer who is responsible for development and implementation of the Covered Entity's policies and procedures
- The privacy and security officer is also the person who will receive initial complaints about potential HIPAA violations
- The position should not be just an empty title

Records Requests

- Patients
- Attorneys
- Court Orders
- Government Agencies

Records Requests Patients

- Patients are entitled to their records with a few exceptions
- Details of the disclosure may be governed by state law
- Attorneys are not considered representatives of the patient for purposes of HIPAA disclosures

Records Requests Attorneys

- Entities May turn over records with
  - Valid Authorization from Patient
  - Pursuant to a valid Judicial or Administrative Order
  - Pursuant to a Subpoena or Discovery requests issued by a judge or administrative tribunal
  - With satisfactory written assurances and including notice to the patient and an opportunity to object

Ninth Circuit Finds HIPAA Limits on Medical Record Copying Fees For Individuals Not Applicable To Law Firm's Request

- *Webb v. Smart Document Solutions, No. 05-56282 (9th Cir. Aug. 27, 2007)*
- Law Firm and Patient/Client sued record production company in a class action suit when company charged more to produce records pursuant to attorney's request than it would have charged if the patient requested the records
- Plaintiff argued it was a violation of HIPAA since Attorneys were acting on behalf of the individual.
- the appeals court noted that HIPAA explicitly restricts fee limitations to requests made by the individual and concretely defines "individual" in a way that excludes others acting on that individual's behalf.
- Note – You need to look at your state's laws, board policies etc.

Compliance
Role of the Attorney

- Attorneys should work in conjunction with the client to draft security policies
- Many Factors must be considered
  - Must be comprehensive and consistent throughout the entity
  - Must integrate the technology, people and processes into the policies
  - Must consider potential disclosures and where feasible have policies preventing them
  - Broad area – requires its own Seminar

ENFORCEMENT

- Private Rights
- Government
  - Criminal
  - Civil

ENFORCEMENT - Private

- There is no private right of action under HIPAA for HIPAA violations
- State law may provide private rights of action for violations of state privacy laws

ENFORCEMENT - Private

- *Acara v. Banks, No. 06-30356* (5th Cir. Nov. 13, 2006)
- In Acara the US District Court dismissed Plaintiff's Complaint after she sued her physician for disclosing PHI in a deposition without her consent.
- In the first Court of Appeals decision on this issue, the 5th Circuit Court of Appeals affirmed the decision finding no express or implied provision in HIPAA creating a private right of action

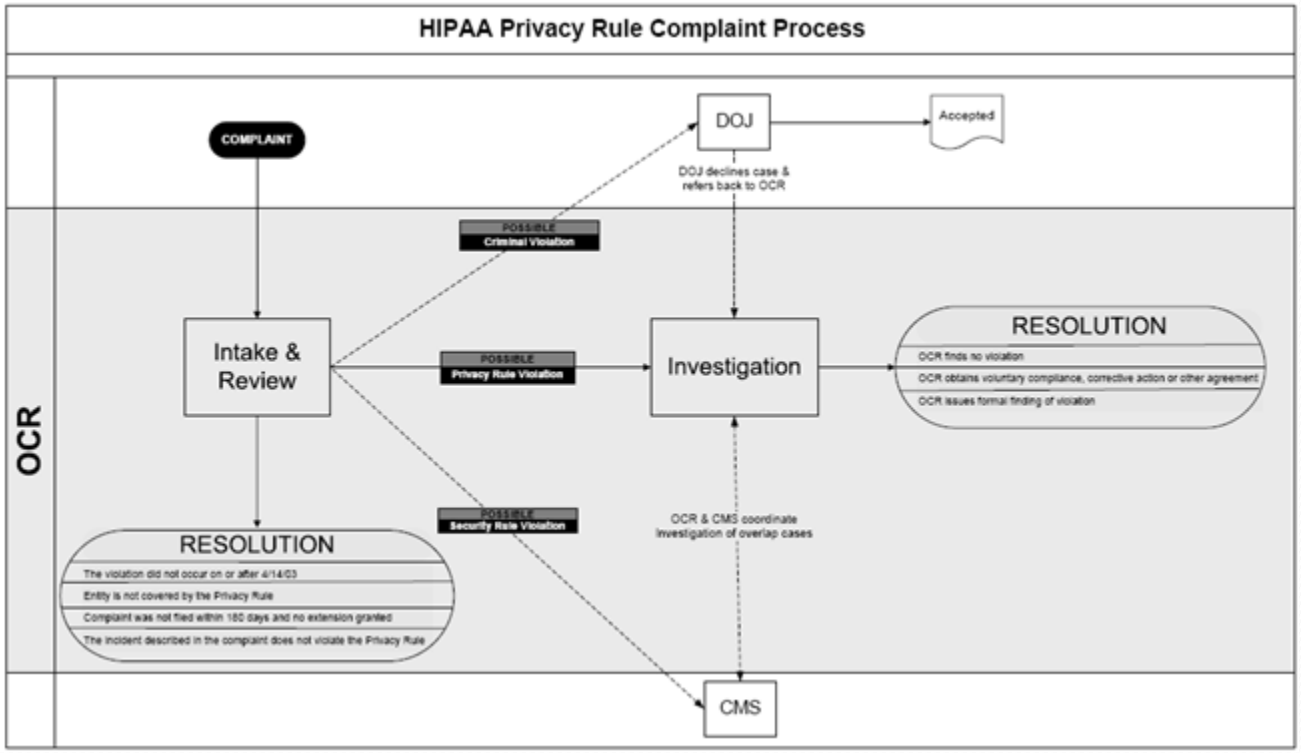
Enforcement - Process

- Complaints start with the entity.
  - Complaint goes to the Privacy Officer
  - Privacy Officer should
    - TAKE SERIOUSLY
    - Investigate
    - Take Appropriate Action
    - Respond to Complainant
    - Take Remedial Action to prevent future similar events
    - DOCUMENT! DOCUMENT! DOCUMENT!
  - How this process is handled may affect whether or not an OCR Complaint is filed.

Enforcement - Government

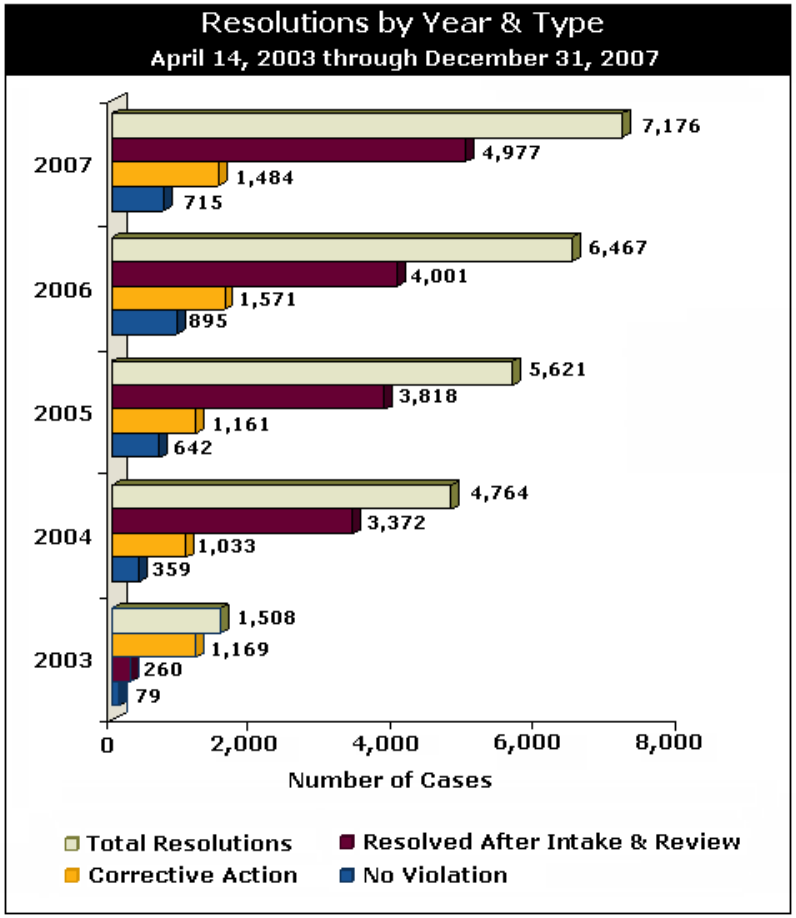
- HHS – Office for Civil Rights – HIPAA
  - www.hhs.gov/ocr/privacy/enforcement
  - Lots of useful information

Enforcement – Government Office for Civil Rights



Enforcement

Office of Civil Rights Statistics



Enforcement Government

- Office for Civil Rights Receives (OCR) Complaint
  - OCR will notify Entity
    - Entity should
      - Notify Compliance Counsel or Outside Counsel
      - Comply with OCR request for Investigation materials
        - Clear everything with legal counsel before disclosing
      - Respond to OCR

Enforcement – Government Continued

- OCR will Investigate
  - Review the information and evidence gathered
- Findings
  - No Violation - Issue a No Action Letter
  - Evidence of Criminal Violation - Turn over to the Department of Justice
  - Non–Compliance – Move Forward

Enforcement – Government Continued

- Criminal Penalties
  - Up to $50,000 and/or imprisonment for up to five years for any person who violates a standard under false pretense. (§1177(b))
  - $250,000 and/or imprisonment of up to ten (10) years for any person who violates any standard with the intent to sell, transfer or use the PHI for a commercial purpose. (§1177(b))

Enforcement – Government Findings of Non-Compliance

- OCR will attempt to resolve informally
  - Voluntary compliance;
  - Corrective action; and/or
  - Resolution agreement
- Most Privacy Rule investigations are concluded to the satisfaction of OCR through these types of resolutions. OCR will notify the entity and complainant of the resolution
  - This is the best way to go if you can

Enforcement – Government Findings of Non-Compliance

- If the matter cannot be resolved informally, OCR will impose Civil Monetary Penalties
  - Entity may submit written evidence of mitigation factors and affirmative defenses
- Civil Monetary Penalties
  - $100.00 per violation up to $25,000.00 for identical violations
  - OCR will consider mitigating factors and affirmative defenses

Enforcement – Government Findings of Non-Compliance

- Notice of Proposed Determination will be sent to Entity explaining
  - Basis in law
  - Findings of Fact
  - Factors in determining amount of penalty
- Entity may appeal
- If the Decision becomes finding the notice is given to public agencies
  - Everyone will have access including state agencies, boards and credentialing entities!

Enforcement – Government Findings of Non-Compliance

- Appeals
  - Within 90 days may request a hearing before the ALJ
    - Off to the Races
    - ALJ may
      - Affirm
      - Reverse
      - Increase or Decrease Penalties

Enforcement – Government Findings of Non-Compliance

- Within 30 days of ALJ decision may appeal to Health and Human Services Department of Appeals Review Board. The Review Board may
  - Decline Review
  - Remand
  - Affirm
  - Reverse
- Within 60 days of Review Board Decision can ask for Reconsideration on basis of Clear Error of Fact or Law

Enforcement – Government Findings of Non-Compliance

- Within 60 days of the Review Board's final decision the entity can appeal to the U.S. Court of Appeals

Enforcement – Fishing

- Secretary is now authorized to conduct compliance reviews without probable cause.

Current and On the Horizon

- What do Covered Entities face now and in the future
  - Constant and repeated disclosures?
    - Accidental
    - Intentional disclosures or peeking at records
      - Celebrities
      - Politicians
      - Ex-Spouses new girlfriend/boyfriend
    - Genetic Information Uses
    - Trade Secret claims
  - HIPAA Audits?
  - Entities will have to be extremely vigilant if they are to avoid HIPAA violations

Conclusion

Patient Rights to Amend Chart

- Under 45 C.F.R. section 164.526 (HIPAA), a patient has the right to have the covered entity amend the record, unless the request falls under an exception (see below). The person must request that the CE amend the medical record. The CE may require that the patient make the request in writing and to provide a reason to support the requested amendment. The CE has 60 days to respond to the request. The CE may deny the request if the CE determines that the record 1) was not created by that CE; 2) is not part of the designated record set; 3) would not be available under sect. 164.524 (which permits patients access to their medical records) or 4) is accurate and complete