Introduction
Topics to be covered
• Background of HIPAA
• Overview and Scope of Coverage Under HIPAA
• PHI: Its Use and Disclosure
• General Rules
• When Is or Isn’t Information Protected
• PHI Identifiers
• Patient Rights
• Administrative Requirements
• Privacy Policies and Procedures
• Practical Examples
• Q&A

Background
• HIPAA (Health Insurance Portability and Accountability Act) Passed in 1996
• Title 1 – Health Insurance Reform (final rule published and in force)
• Title 2 – Administrative Simplification
  – Standards for electronic health care transactions
  – National Identifiers
  – Security and Privacy
Electronic Standards

- All electronic transactions must be in prescribed formats by October 16, 2002
- An automatic extension is available until October 15, 2003 by filing the model compliance plan
- The request for the extension must be filed by October 15, 2002
- The form is available at:

HIPAA

- Overview of Privacy Rules: Health Insurance Portability and Accountability Act (HIPAA)
  - Sets standards for privacy of individually identifiable health information
  - Allows information to be used and shared for the purposes of treatment, payment and health care operations (TPO)
  - Requires notification or authorization for use and disclosure
  - Creates processes to let patients know how information is to be used, ensures patients have access to their information and an ability to correct inaccuracies.
  - Requires health plans and providers to maintain administrative and physical safeguards on information

HIPAA

- Scope of HIPAA
  - Covers all providers of any size from University Medical Centers to solo physicians
  - Health Plans
  - Health care clearing houses
  - Business agents of the above who have legitimate need to have information (consultants, employees, billing agencies)
  
  Your practice is covered!
  And you have to help make it work!
**HIPAA**

- **Protected Health Information (PHI)**
  - All information relating to the diagnosis and treatment of a patient that is individually identifiable
  - Originally, this was only to apply to electronic data. In the final rule it has been applied to all information
  - HIPAA protects the information itself for privacy, it does not make patients anonymous!

---

**HIPAA**

- **General rules**
  - Providers and others are prohibited from using or disclosing PHI except when authorized by the patient or for treatment, payment or health care operations (TPO.)
  - TPO
    - This is the normal, everyday business of conducting the office and seeing patients, referring them for tests and other care and getting paid for the work you do.
    - It means staff can look at the chart, you can send needed information to other providers and you can provide a payer with information on the services and

---

**HIPAA**

- **General rules**
  - Every patient must be notified of their privacy rights, the practice's privacy policies and how PHI will be used. Patients must acknowledge this notification in writing.
    - This means the practice must have privacy policies that describe the patient's rights
    - Patients must have an opportunity to see your policies and they must acknowledge in writing they have received this notification
HIPAA

• General rules
  – The amount of information to be used or disclosed should be the minimum that accomplishes the purpose.
  ∙ Minimum Necessary Standard – you must make reasonable efforts to limit the PHI to the minimum necessary to meet the purpose or request.
  ∙ Disclosures to or requests from other providers for treatment are an exception to this rule.
  ∙ Disclosures to or requests from the person for their own PHI is an exception to the rule
  ∙ Practices must identify the staff who need access to the PHI

HIPAA

• General rules - continued
  – Business associates may have access to protected information under a contract with the provider. The agent then has the same responsibilities as the provider
  ∙ If you have a billing service that needs to see PHI as part of their billing they are an agent
  ∙ If you engage a consultant to review charts or engage in other practice work such as audits or QI/QA, they are an associate and are covered under the rules.
  ∙ Collection agencies are business associates

HIPAA

• General rules - continued
  – Uses and disclosures are permitted – not required except by law.
  – Only two disclosures are required:
    ∙ Disclosure to the patient on request
    ∙ Disclosures required by law (subpoenas, federal payments, etc)
  – Information will be protected for two years following the death of the patient
### HIPAA

#### When Is Personal Information Protected?
- Does the information identify the patient or can it be used to identify the patient?
- Does the information relate to the past, present or future health, treatment or payment for provision of services?
- Was the information created by a health care provider, health plan, employer, life insurer, public health agency, school, health care clearinghouse?

#### When Is Personal Information Not Protected?
- Is the information part of an education record (Family Education and Privacy Act)?
- Is the information on a student older than 18 created or maintained by the provider and only available to the provider or another provider designated by the student?
- Is the information contained in employment records of the practice as opposed to the medical records the practice may have on employees?

#### When Can PHI be Used or Disclosed?
- When the disclosure is to the patient
- For treatment, payment or health care operations involving the patient
- Incident to a use that is permitted
- When the practice receives a valid authorization
- When the practice has obtained the patient’s oral agreement
- When the law specifically does not not require authorization
HIPAA

• Permissible Uses and Disclosures
  - Quality Assurance Activities
  - Public health and emergencies affecting life or safety
  - Research
  - Judicial hearings
  - Law enforcement
  - Information to next-of-kin
  - Identification of a body or cause of death
  - Government Health Data Systems
  - Facilities Data Systems
  - Financial entities for processing claims
  - Where mandated by law

18 Ways to Identify A Patient

1. Names
2. Addresses
3. Dates relating to the patient
4. Telephone numbers
5. Fax numbers
6. E-mail addresses
7. Social Security #
8. Medical record #
9. Health Plan ID #
10. Account numbers
11. License numbers
12. Vehicle identification #
13. Device identifiers
14. Web address – URL
15. IP address
16. Biometric identifiers
17. Full face images
18. Any other unique identifying number, characteristic or code

HIPAA

• Individual Rights
  - The right to receive written notice of the information practices of providers and health plans
    • The notice must describe the types of uses and disclosures the provider would make with the information
  - The right to access protected information
  - The right to request amendment of records
  - The right to receive an accounting of when protected information has been disclosed
HIPAA

• Administrative Requirements
  - Providers must develop administrative policies and procedures to protect information and the rights of the patient
  - Maintain documentation of the policies and procedures including how information is used, who can get it and for what purpose
  - Providers must:
    • Designate a privacy official
    • Provide training to physicians and staff
    • Implement appropriate safeguards
    • Create a complaint mechanism
    • Develop sanctions for employees and business associates who violate the policies and procedures

Privacy Policies

• Use and disclosure
  - Who can use it and how and to whom it may be disclosed
• Minimum Necessary
  - Describes typical uses of PHI
• Incidental Disclosures
  - Cannot be reasonably prevented but good faith attempts are made to minimize the disclosure

Privacy Policies

• Procedures for disclosing PHI
  - What is required from the requestor, how is it transmitted and what must be documented in a permanent record
• Consent and Notification
  - Notification of privacy policy
  - Consent to use and disclose PHI for TPO
  - Written acknowledgement of receipt of notification
Privacy Policies

• Authorization
  - Not required for TPO
  - Research purposes
  - Marketing purposes other than face-to-face presentations from the doctor or nominal token promotional gifts
  - Release of PHI to entities not covered by HIPAA such as communications to schools and employers
  - Special authorization for psychotherapy notes

• Authorization and consents
  - After the fact authorizations and consents in emergencies
    • Not possible or practical for the physician to be carrying consents and authorizations
    • Forward the information and the forms for consent and/or authorization as soon as practical after the initial encounter
    • Tip: Have proof of mailing for after-the-fact notifications

• Uses and Disclosures Involving Family and Friends
  - Does not require an authorization but is not required unless directly requested by patient
  - May also use PHI to notify a family member or responsible person of the patient’s location or condition
    • Patient must be able to provide consent or an opportunity to object and there is no objection or reasonably infer the patient has no objection such as by being accompanied by a friend or family member
Privacy Policies

• Dealing With Minors (or Personal Representatives)
  - The parent/guardian or personal representative may provide all consents and notifications on the patient's behalf
  - Two exceptions:
    • If there is a reasonable belief that the patient may be subjected to abuse by the requestor
    • If, under state law, the minor is emancipated or the treatment concerns matters over which the state permits the minor to obtain health care without parental consent

Privacy Policies

• Verification of Identity
  - Employees must verify the identity and authority of persons making requests for PHI
  - Policies should describe minimal forms of proper identification (which may include subpoenas)
  - Information should be provided in a secure and confidential manner
  - If you have a good faith belief that releasing the PHI will avert harm to the patient or the public you may release the information.

Privacy Policies

• Business Associates
  - Tip: Make a list of all entities you believe are business associates and request a new HIPAA compliant contract
  - The practice is not liable for the privacy violations of its business associates but it must exercise appropriate safeguards and have mechanisms to act if it becomes aware of such violations
  - Model contract language is available from CMS
Preemption of State Law

- Generally, HIPAA rules prevail where state law is silent.
- HIPAA prevails if state law is less stringent.
- State law prevails if it is more stringent.
- Most rules dealing with privacy for minors is deferred to states under HIPAA.
- State law summaries on privacy are available at:
  http://www.healthprivacy.org/info-url_nocat2304/info-url_nocat.htm

Practical Examples

# 1. The patient is a minor and the patient’s mother wants to pick up a prescription for the patient.

# 2. A pharmacy calls wanting authorization to re-fill a prescription.
# 3. The patient is being referred to another practice and a copy of the most recent notes and lab findings are requested by the practice. Later they ask for the full chart.

# 4. The patient is elderly and the patient's adult daughter contacts the practice to get more information on her mother's condition, treatment and plans.

# 5. A father of a newborn wants medical records of the child but those records contain information on the mother as well.
Practical Examples

# 6. A patient indicates in a conversation with the doctor she heard another patient, who is a friend, is going to have some tests ordered and wonders if she is going to be okay.

Practical Examples

# 7. A patient requests an accounting of disclosures of PHI prior to April 15, 2003. ...After April 15, 2003

Practical Examples

# 8. The practice has a sign-in sheet listing the names of all patients seen that day at the front desk. Anyone signing in can see it.
Practical Examples

# 9. Lists of patients, including the reason they are being seen, are posted around the office as the daily schedule.

Summary

- In one sense HIPAA privacy rules are nothing new. You have always treated information confidentially. Now there are uniform standards.
- Common sense and good judgment will almost always work if you are keeping the best interests of the patient in mind.
- If in doubt, talk to your manager or supervisor.

Thank you for participating in this program from Economedix!

For Questions please e-mail to...

toughrey@economedix.com
Coding & Reimbursement
Financial Management
Human Resources
Patient Flow & Marketing
Compliance & Medicare

http://YourMedPractice.com