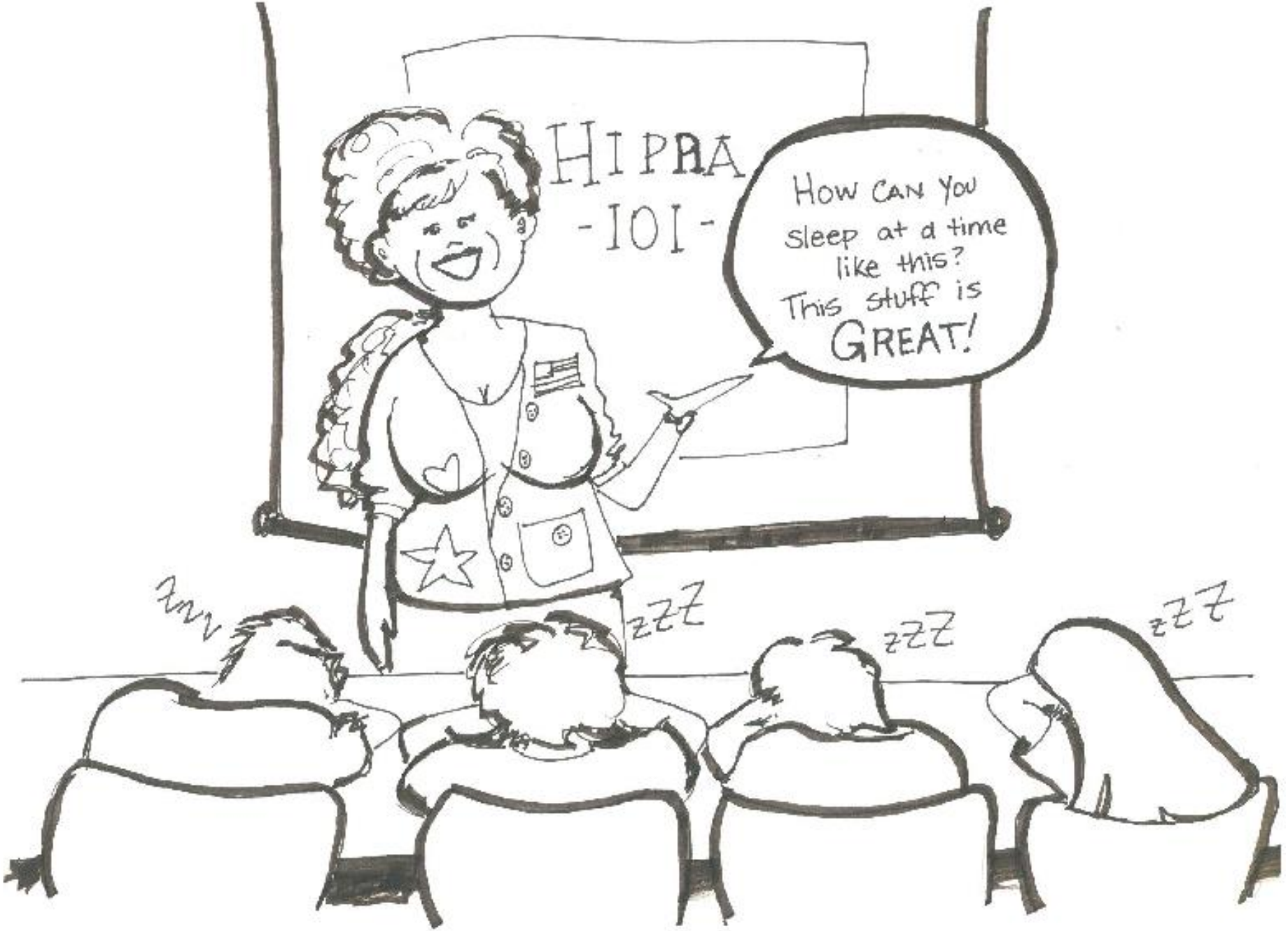

HIPAA
-101-
How can you sleep at a time like this? This stuff is GREAT!
zzz
zzz
zzz
zzz

HIPAA

Health Insurance Portability and Accountability Act

Connie Bryant

Regulatory Compliance Officer

Montgomery County Hospital District

Greg Hudson

Attorney

Hudson and O'Leary, L.L.P.

Basic requirements of HIPAA

- NOTICE OF PRIVACY PRACTICE--Notifying patients about their rights and how information can be used
- Must create policies and privacy procedures
- Must train employees how to handle PHI
- Privacy Officer: individual responsible for seeing that the privacy procedures are adopted and followed
- Protect PHI: Securing patient records so that they are not readily available to those who do not need them.
- Share PHI with necessary vendors through Business Associate Agreements

WHAT DOES HIPAA STAND FOR?

- **HIPAA stands for:**
- Health Industry Paying All Attorneys
- Highly Intricate Paperwork in Abundant Amounts
- Health Insurance Pain in the Ass Act
- High Income Potential for Aggressive Attorneys
- Having Impact Past All Assumptions
- Huge Increase in Paperwork and Aggravation Act

Case 1

Someone calls your office and wants to give you information regarding one of your clients—you advise them you can't receive protected health information from anyone except the client—please ask them to call us.

Is this the correct response?

Case 1

- **HIPAA regulates the release of information NOT the receipt of information.**

CASE 2

You receive a subpoena from a law firm. It list your client as a party in a lawsuit and request information regarding payments made for their healthcare.

Should you release the information?

What if they were not named as a party in the lawsuit.

CASE 2

If they are a party in the lawsuit there was an AG opinion that clarified it is acceptable to release the information.

If they are NOT a party you need an authorization unless it is court ordered.

HINT: May be a civil case and someone else may be a better payor—be a detective!

KNOCK, KNOCK

Who's there?

HIPAA.

HIPAA who?

Sorry, I'm not allowed to disclose that information.

CASE 3

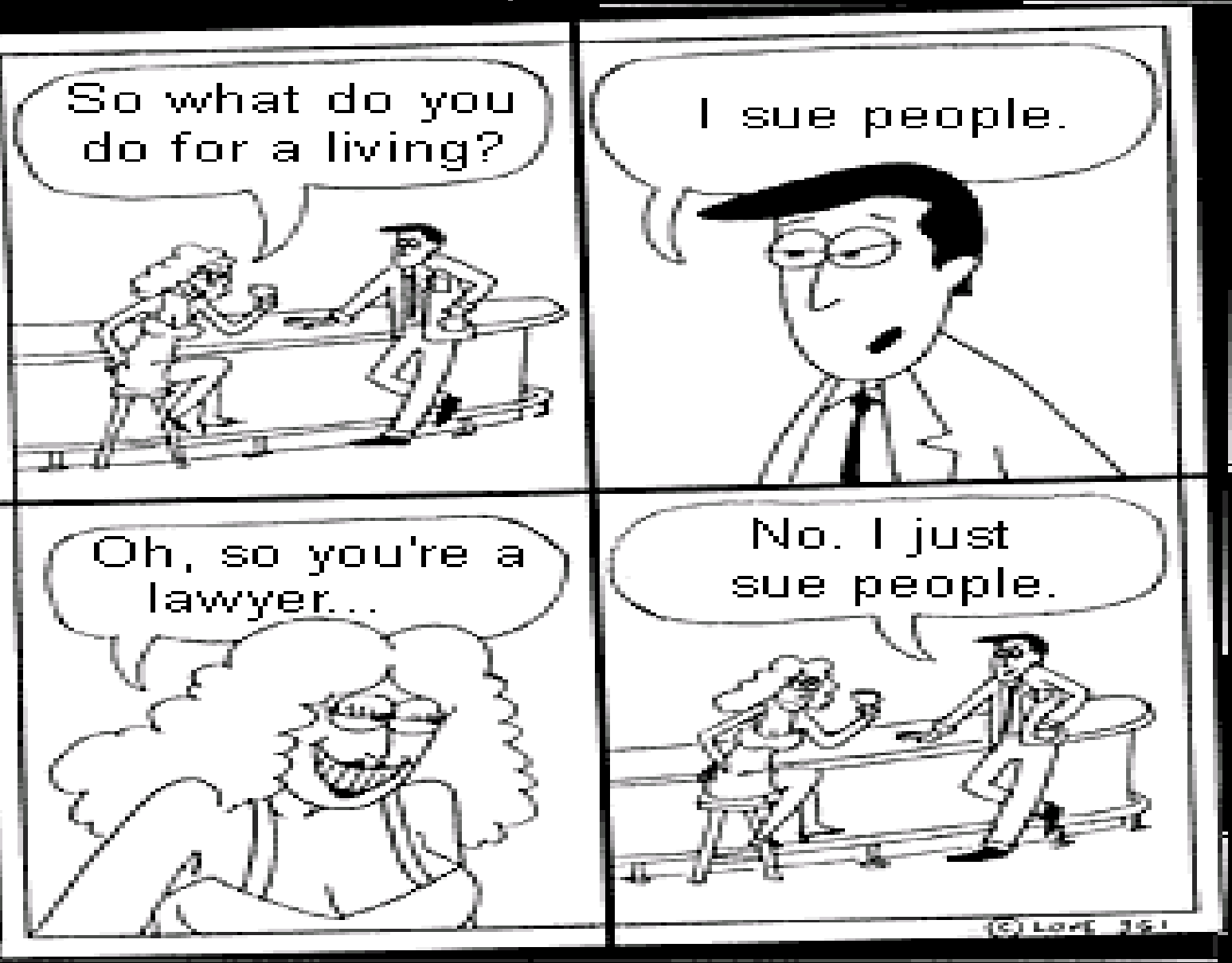
A client contacts you and request their record be amended.

Do you have to amend the record?

Case 3

- HIPAA gives the patient the right to request an amendment.
  - Must respond within 30 days
  - Should respond in writing
  - If the information in the record is factual—deny request in writing
  - Denied request may require that you release patient request for amendment with future record request

SNAPSHOTS by Jessica Lang



HIPAA – NO PRIVATE RIGHT OF ACTION

- Recent case in the Fifth Circuit held that persons cannot sue for violations of HIPAA

Open Records vs. Protected Health Information

- Can the public have a list of everyone who receives coverage?
- Can the public have a list of how much money was spent by your program on a specific medication?
- When in doubt…AG Determination
  - *What is that and how do I do it?*

AG Opinion

- Attorney general determines whether information is subject to disclosure.
  - Governmental body must provide to the requestor within 10 business days of receiving the request:
    - A written statement that it wishes to withhold the information and has asked for an AG opinion.
    - Copy of the written opinion request to the AG.

AG Opinion

- Governmental body that requests an attorney general decision must within a reasonable time but not later than the 15th business day after receiving the request submit to the AG:
  - Written comments stating the reasons for withholding the information (reason for withholding will be the request involves a third parties privacy)
  - copy of the written request information or representative samples.
- Information presumed public if submissions and notifications are not timely filed.

HIPAA DOESN'T AFFORD INDEPENDENT PROTECTION UNDER THE TEXAS PUBLIC INFORMATION ACT

- Normally, information protected by other law isn't subject to the Texas Public Information Act
- But the A.G. has ruled that HIPAA is not other law, so as to protect PHI (*Tex. Att'y Gen. ORD – 681 (2004*))
- Check State confidentiality laws instead that may protect some of the PHI

ATTORNEY GENERAL OF TEXAS
GREG ABBOTT

February 13, 2004

Senator Robert Duncan Chairman Senate Committee on Jurisprudence P.O. Box 12068 Austin, Texas 78711	Open Records Decision No. 681 Re: Questions concerning the applicability of the HIPAA Privacy Rule and state law to health information subject to the Public Information Act, chapter 552 of the Texas Government Code (ORQ-65).

SUMMARY

When a covered entity that is a governmental body subject to the PIA is presented with a request under the PIA for protected health information from a member of the public, it must evaluate each disclosure under the PIA as it does now under current procedures. The Privacy Rule does not make information confidential for the purpose of section 552.101 of the Government Code. A governmental body that is subject to both the PIA and the Privacy Rule must comply with the Privacy Rule in disclosing protected health information that is not requested under the PIA.

Beware of the HIPAA Security Rule

- **Applicability and Scope**

  The Security standards apply to all individually identifiable health information that is in electronic form, whether it is being stored or transmitted. This includes all administrative and financial healthcare transactions covered by the HIPAA Transactions Standards Rule, including internal transmissions. Health information that is on paper or oral is not covered. All healthcare providers, health plans, or clearinghouses that electronically store or transmit individual health information must comply.

Beware of the HIPAA Security Rule

- **Security Threats**

  The Security Rule focuses both on external and internal security threats and vulnerabilities. Threats from "outsiders" include breaking through network firewalls, e-mail attacks through interception or viruses, compromise of passwords, posing as organization "insiders,"computer viruses, and modem number prefix scanning. These activities can result in denial of service, such as the disruption of information flow by "crashing" or overloading critical computer servers. The outsider may steal and misuse proprietary information, including individual health information. Attacks can also affect the integrity of information, by corrupting data that is being transmitted.

Beware of the HIPAA Security Rule

Internal threats are of equal concern, and are far more likely to occur according to many security experts. Organizations must protect against careless staff or others who are unaware of security issues, and curious or malicious insiders who deliberately take advantage of system vulnerabilities to access and misuse personal health information.

http://www.hipaadvisory.com/regs/securityoverview.htm

HIPAA Security Rule Compliance

- **October 13, 2006 Latest HIPAA Survey Finds Security Rule Compliance Remains Low** Most “covered entities” have complied to some extent with most of the HIPAA regulations, but Security Rule compliance remains low among healthcare providers, according to results of the latest US Healthcare Industry HIPAA Survey sponsored by Phoenix Health Systems and the Healthcare Information and Management Systems Society (HIMSS). Though the deadline for compliance with the HIPAA Security Rule passed over a year ago, 80% of payers and only 56% of providers who responded to the Summer 2006 Survey have implemented the Security standards. Of those claiming full compliance with the Security Rule, gaps remain; many “compliant” Providers and Payers could not confirm that they had implemented all key Security standards. The twice-yearly survey is in its seventh consecutive year of tracking and reporting on the status of HIPAA compliance within the healthcare industry.

http://www.hipaadvisory.com/news/recentnews.htm

Did you forget something?

What About Emergencies

DEPARTMENT OF HEALTH & HUMAN SERVICES OFFICE OF THE SECRETARY

Director
Office for Civil Rights
200 Independence Ave., SW Rm 509F
Washington, DC 20201

September 2, 2005

U.S. Department of Health and Human Services Office for Civil Rights

HURRICANE KATRINA BULLETIN:
HIPAA PRIVACY and DISCLOSURES IN EMERGENCY SITUATIONS

- ✓ **TREATMENT.** ***Health care providers can share patient information as necessary to provide treatment***.

    - *Treatment* includes
        - sharing information with other providers (including hospitals and clinics),
        - referring patients for treatment (including linking patients with available providers in areas where the patients have relocated), and
        - coordinating patient care with others (such as emergency relief workers or others that can help in finding patients appropriate health services).

    - Providers can also share patient information to the extent necessary to seek payment for these health care services.

- ✓ **NOTIFICATION.** ***Health care providers can share patient information as necessary to identify, locate and notify family members, guardians, or anyone else responsible for the individual's care of the individual's location, general condition, or death.***

    - The health care provider should get verbal permission from individuals, when possible; but, if the individual is incapacitated or not available, providers may share information for these purposes if, in their professional judgment, doing so is in the patient's best interest.

        - Thus, when necessary, the hospital may notify the police, the press, or the public at large to the extent necessary to help locate, identify or otherwise

notify family members and others as to the location and general condition of their loved ones.

- In addition, when a health care provider is sharing information with disaster relief organizations that, like the American Red Cross, are authorized by law or by their charters to assist in disaster relief efforts, it is unnecessary to obtain a patient's permission to share the information if doing so would interfere with the organization's ability to respond to the emergency.

IMMINENT DANGER. Providers can share patient information with anyone as necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public -- consistent with applicable law and the provider's standards of ethical conduct.

FACILITY DIRECTORY. Health care facilities maintaining a directory of patients can tell people who call or ask about individuals whether the individual is at the facility, their location in the facility, and general condition.

rse, the HIPAA Privacy Rule does not apply to disclosures if they are not made by entities d by the Privacy Rule. Thus, for instance, the HIPAA Privacy Rule does not restrict the can Red Cross from sharing patient information.

http://www.hhs.gov/ocr/hipaa/KATRINAnHIPAA.pdf

PENALTY FOR HIPAA VIOLATIONS – (FEDERAL)

- Complaint driven
- OCR may impose monetary penalties up to $100/violation or $25,000
- Criminal Penalties are possible
  - Up to $50,000 and one year in prison to $100,000 and five years in prison
  - $250,000 and 10 years in prison if offense includes intent to sell, personal gain or malicious harm

State laws

- Don’t forget the Texas Health and Safety Code also protects patient privacy
- Chapter 181 – Tex. Health & Safety Code
- Section 241.152 – Tex. Health & Safety Code (Hospitals)
- Occupations Code, Title 3, Chapter 159, "Physician-Patient Communication”


RECOMMENDED PENALTY
FOR UNAUTHORIZED
RELEASE OF PHI

State laws

- **Medical Record Privacy 'Above the Norm' in Texas, Says Study**
  Vivi Hoang WASHINGTON _ Patients in Texas have greater privacy protection for their medical records than many other Americans, say researchers.

  But, Texans still need more safeguards, added Joy Pritts of the Health Privacy Project based at Georgetown University.

  Texas laws on medical privacy are "above the norm" among the states, said Pritts. "Some of the things that Texas has in its laws are very consumer-oriented," she said.

  On Tuesday, the Health Privacy Project released a state-by-state report on health privacy laws. **Texas, the report says, does not have one grand law that forbids the disclosure of confidential patient information. Rather, the state has multiple laws that spell out what specific health care groups—doctors, hospitals, health maintenance organizations—can release**.

http://www.shfwire.com/node/3091

TEXAS LAW – HIPAA EQUIVALENT

SUBTITLE I. MEDICAL RECORDS
CHAPTER 181. MEDICAL RECORDS PRIVACY
SUBCHAPTER A. GENERAL PROVISIONS

§ 181.001. DEFINITIONS. (a) Unless otherwise defined in this chapter, each term that is used in this chapter has the meaning assigned by the Health Insurance Portability and Accountability Act and Privacy Standards. (b) In this chapter:

(2) "Covered entity" means any person who: (A) for commercial, financial, or professional gain, monetary fees, or dues, or on a cooperative, nonprofit, or pro bono basis, engages, in whole or in part, and with real or constructive knowledge, in the practice of assembling, collecting, analyzing, using, evaluating, storing, or transmitting protected health information. **The term includes a business associate, health care payer, governmental unit, information or computer management entity, school, health researcher, health care facility, clinic, health care provider**, or person who maintains an Internet site; (B) comes into possession of protected health information; (C) obtains or stores protected health information under this chapter; or (D) is an employee, agent, or contractor of a person described by Paragraph (A), (B), or (C) insofar as the employee, agent, or contractor creates, receives, obtains, maintains, uses, or transmits protected health information.

TEXAS LAW – HIPAA EQUIVALENT

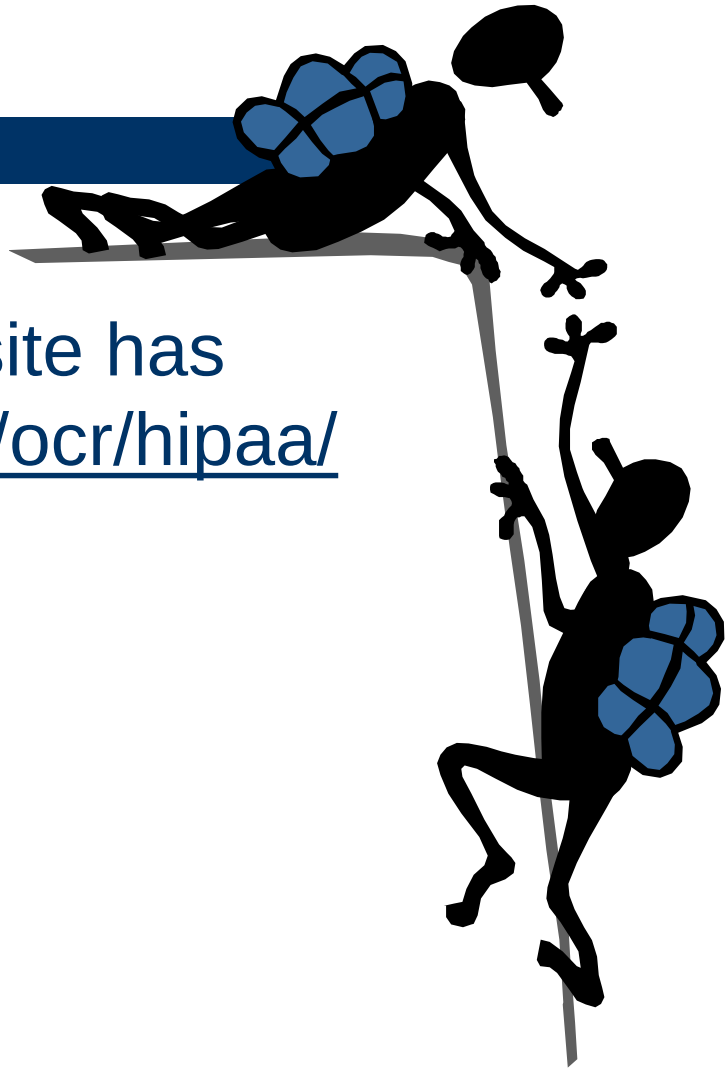
§ 181.005. DUTIES OF THE COMMISSIONER.
(a) The commissioner shall administer this chapter and may adopt rules consistent with the Health Insurance Portability and Accountability Act and Privacy Standards to administer this chapter.

TEXAS LAW – HIPAA EQUIVALENT - PENALTIES

- § 181.201. INJUNCTIVE RELIEF; CIVIL PENALTY. (a) The attorney general may institute an action for injunctive relief to restrain a violation of this chapter. (b) In addition to the injunctive relief provided by Subsection (a), the attorney general may institute an action for civil penalties against a covered entity for a violation of this chapter. A civil penalty assessed under this section may not exceed $3,000 for each violation. (c) If the court in which an action under Subsection (b) is pending finds that the violations have occurred with a frequency as to constitute a pattern or practice, the court may assess a civil penalty not to exceed ***$250,000***.

- OUCH!!!

HELP!



- Office of Civil Rights website has FAQ's http://www.hhs.gov/ocr/hipaa/
- Information Line for OCR
  866-627-7748
- OCR Privacy List Serve
- HIPAA Assistance line:
  214-767-4057

HIPAA

Health Insurance Portability and Accountability Act

Connie Bryant

Regulatory Compliance Officer

Montgomery County Hospital District

Greg Hudson

Attorney

Hudson and O'Leary, L.L.P.