NIXON PEABODY LLP

High-Stakes Medical Privacy Litigation: The Top HIPAA Threats and How To Avoid Them

Fifth National HIPAA Summit
Baltimore, MD
November 1, 2002

Sal Colletti, Esq., Pfizer Inc.
Ray Gustini, Esq., Nixon Peabody LLP
Leigh-Ann Patterson, Esq., Nixon Peabody LLP

Preventive Law

National Center for Biotechnology Law:

"Using the analogy with preventive medicine, preventive law is the legal specialty of preventing the disease of litigation. Litigation is a serious disease that leaves its victims financially and emotionally weakened and, in some cases, may lead to their economic demise…"

Preventive Law

"[Litigation] is a contagious disease characterized by a latent state with intermittent crises (individual suits). Symptomatic treatment of the crisis phase may lead to a remission, but the disease usually recurs in a more serious form. ... The disease cannot be cured, but it can be controlled by carefully monitored therapy and regular checkups."

Overview of Session

We're going to discuss three things:

First: "Litigation 101"

- **What is high-stakes litigation?**
- **Why should you be concerned about it?**
- **How do HIPAA and medical privacy issues lend themselves to high-stakes litigation?**

Overview of Session

Second: The Top HIPAA Threats

- **"HIPAA 101" – brief overview of provisions discussed in this session**
- **Low-stakes medical privacy exposure**
- **High-stakes medical privacy exposure:**
  - **(1) Inadvertent mass disclosure due to poor security**
  - **(2) Failure to follow one's own privacy policies and procedures**
  - **(3) Medical data abuses or breaches by business associates**

Overview of Session

Third: How To Minimize the Risk of Future HIPAA Litigation

(a.k.a. How to Reduce Your Chances Of Becoming The First HIPAA Litigation Posterchild)

- **Think differently about HIPAA and Medical Privacy Issues**
- **Build a Strong Privacy Foundation**
- **Training, Awareness, and Self-Audits**

"Litigation 101"

A. What is High-Stakes Litigation?

"Litigation 101"

Three general categories of personal injury lawsuits:

- Low-Stakes Litigation
- High-Stakes Litigation
- Mass Torts Litigation

"Litigation 101"

Low-Stakes Litigation

- Largest category
- A single plaintiff
- Injured in a typical or common way
- Minor injuries
- Seeks compensation for injuries

"Litigation 101"

High-Stakes Litigation

- **Many plaintiffs; national class action**
- **Injured in a similar way by one or more defendants**
- **Seek compensation <u>PLUS</u> DETERRENCE, i.e. punitive damages to deter defendant from doing it again = $$$$$$**

"Litigation 101"

Mass Tort Litigation

- **Smallest category**
- **Many plaintiffs; consolidated class actions**
- **All injured same way by single product, i.e. Dalkon shield cases**
- **Seek compensation PLUS DETERRENCE**

"Litigation 101"

B. Why Should You Be Concerned About It?

It's the fastest growing type of lawsuit in the state court systems. Plaintiffs are lining the court steps to join high-stakes class actions.

"Litigation 101"

The stakes are higher because of the deterrence factor. "Make the defendant pay" mentality.

"Litigation 101"

Risk of

HUGE

punitive damage

award

"Litigation 101"

C. How Do HIPAA and Medical Privacy Issues Lend Themselves to High-Stakes Litigation?

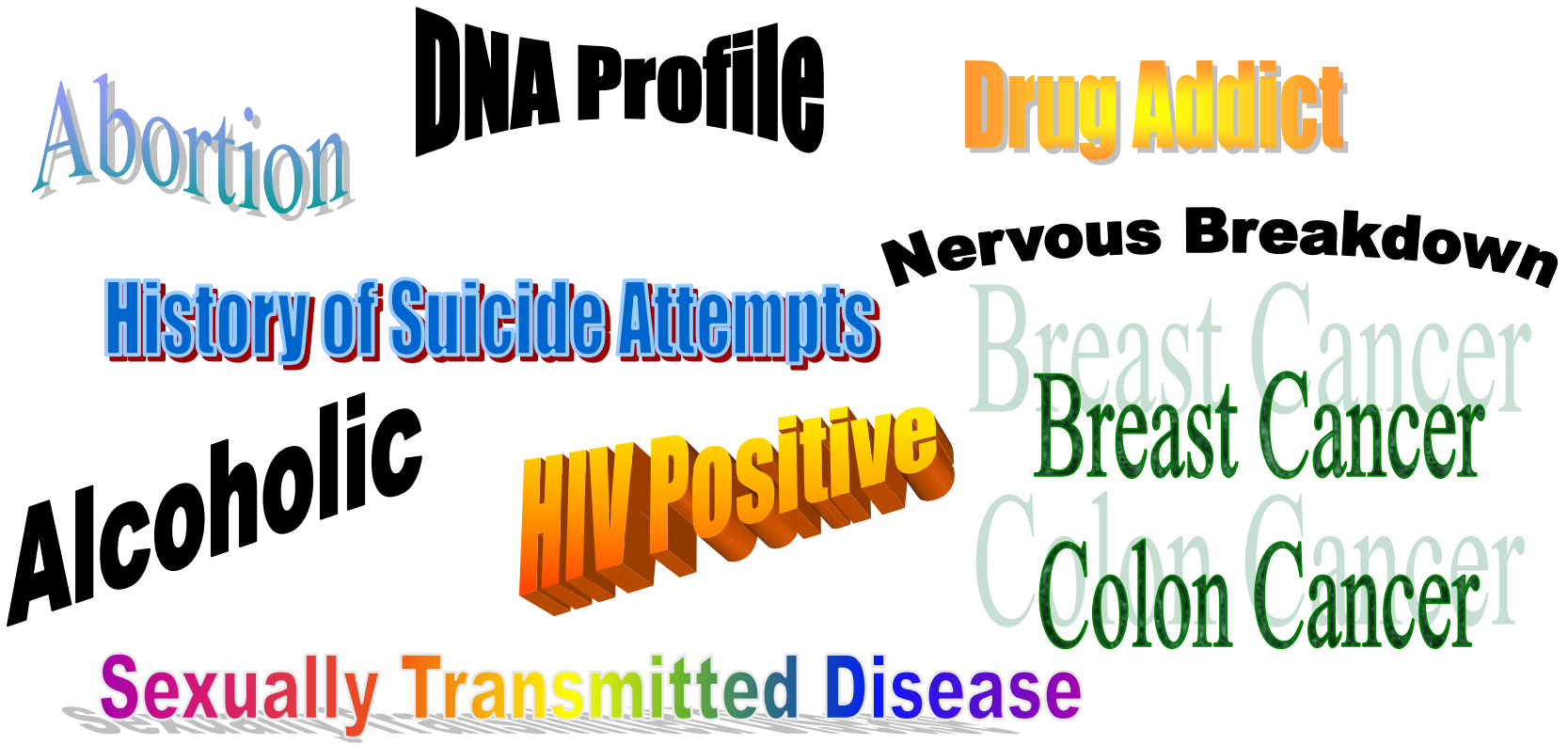
- Ease of Intentional/Accidental Disclosure
- Sensitivity of the Information

"Litigation 101"

Ease of disclosure in the high tech world of HIPAA

"Litigation 101"

Sensitivity of the information:



"Litigation 101"

Sensitivity of the information

leads to emotionally-charged

plaintiffs . . .

which leads to

high-stakes deterrence:

$$$$$$$$$$$$$$$$$$$$$

"Litigation 101"

What are Plaintiffs' lawyers saying about HIPAA litigation?

- **It's the next "Tobacco Litigation"**
- **Better than "Asbestos Litigation"**
- **Move over "Breast Implant Litigation"**

The Top HIPAA Threats

A. "HIPAA 101" – Brief Overview of provisions discussed in this session

- Covered entity
- Business associates
- PHI
- Consent

The Top HIPAA Threats

B. Low-Stakes Medical Privacy Cases

Low-Stakes Medical Privacy Cases – single plaintiff, low damages

- **Washington Hospital Center:** A patient sued the Washington Hospital Center in Washington, DC, when a hospital employee revealed to the patient's co-workers his HIV-positive status. The patient was awarded $25,000 in damages for invasion of privacy.
- **Waukesha, Wisconsin**: A patient who had overdosed and was treated by an emergency medical technician in Waukesha, Wisconsin, sued the EMT for disclosing the overdose to the patient's co-workers. The patient was awarded $3,000 in damages for invasion of privacy.
- **Emory School of Medicine:** A nurse sued the Emory School of Medicine when her supervisor posed as her treating physician and wrongfully accessed her medical records without permission. This suit is still pending.

Low-Stakes Medical Privacy Cases – single plaintiff, low damages

- **San Francisco law firm:** An employee sued a San Francisco law firm that represented her employer, claiming that the law firm wrongfully shared information, including a psychiatric evaluation, about her workers' compensation claim with one of the plaintiff's co-workers. This suit is still pending.

- **Johns Hopkins Hospital:** A patient of Johns Hopkins Hospital sued the hospital for $12 million, alleging that the hospital wrongfully released his medical records to a former friend and business partner. The court held that Johns Hopkins was not liable because it did not knowingly release the information to the former friend. An appeal is presently pending.

Low-Stakes Medical Privacy Cases – single plaintiff, low damages

- **Significance?**

  They're laying the groundwork -- some of these low-stakes cases are beginning to incorporate HIPAA into their state-law claims and theories of liability for invasion of privacy, notwithstanding the fact that HIPAA does not create a private right of action. One Court recently recognized HIPAA as setting a national "standard of care."

C. High-Stakes Medical Privacy Exposure

How might the first case happen?

- **Inadvertent Mass Disclosure Caused by Poor Security Measures**

The Existing HIPAA Security Requirement

- Even though a final security rule has not yet been published, a security standard is in existence right now in the underlying HIPAA statute.
- HIPAA's standard for security is found at 42 U.S.C. §1320d-2(d)(2):

The Existing HIPAA Security Requirement

42 U.S.C. §1320d-2(d)(2):

Safeguards

"Each [covered entity] who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards –

(A) to ensure the integrity and confidentiality of the information;

(B) to protect against any reasonably anticipated –

(i) threats or hazards to the security or integrity of the information; and

(ii) unauthorized uses or disclosures of the information; and

(C) otherwise to ensure compliance with this part by the officers and employees of such person."

How Plaintiffs' Lawyers Might Use The Security Rule As Basis For Lawsuit

Not the way you think:

- No private right of action
- Solid body of federal court caselaw so holding:
  - Means v. Independent Life and Acc. Ins. Co., 963 F. Supp. 1131 (M.D.Ala. 1997)
  - Wright v. Combined Insurance Co. of America, 959 F. Supp. 356 (N.D. Miss. 1997)
  - Brock v. Provident America Ins. Co., 144 F. Supp.2d 652 (N.D.Tex. 2001)
  - Dixie O'Donnell v. Blue Cross Blue Shield of Wyoming, 173 F. Supp. 2d 1176 (Dst.Wy., 2001)
- Means plaintiffs can't sue you for violating HIPAA

How Plaintiffs' Lawyers Might Use The Security Rule As Basis For Lawsuit

In connection with a state law negligence claim by patients for disclosure of PHI due to a security breach.

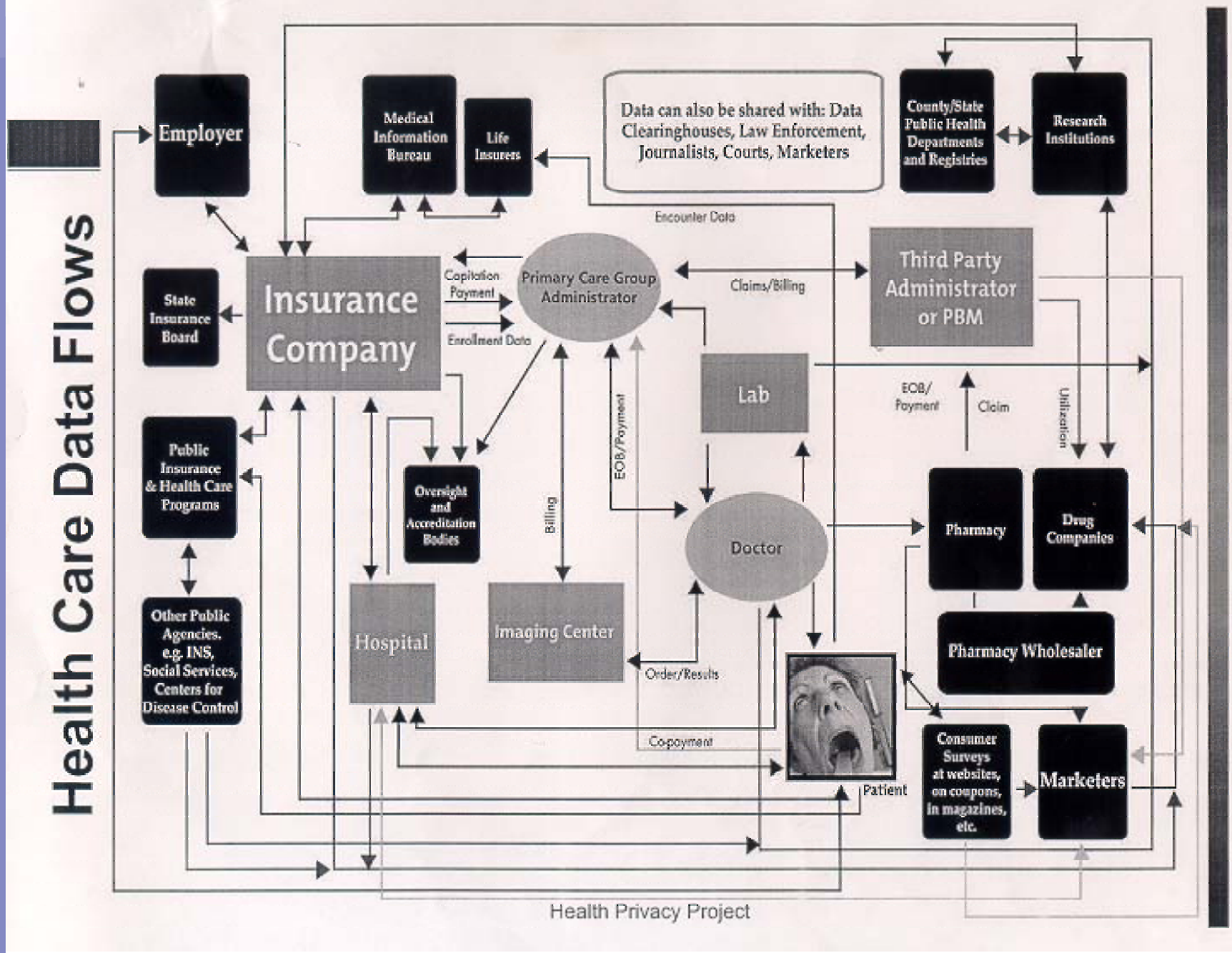
Other potential causes of action:

- Negligent disclosure of PHI
- Intentional revelation of PHI by employee
- Any state statute giving rise to a right of action for breach of confidentiality
- Inadequate policies and procedures
- Negligent supervision and training
- Negligent/intentional infliction of emotional distress

These causes of action and theories of liability appeared in the complaint filed in Jane Doe v. Community Health Plan Kaiser Corp., No. 8529 (N.Y.App. Div. 05/11/2000) (medical records clerk improperly released records).

How and Where a Security Breach Might Occur:

It depends on who you are and what you do.



How and Where a Security Breach Might Occur

Some possibilities:

- Computer security – workstations, laptops, and mobile medical devices
- Communications security
- Physical security: access to premises, equipment, people, data
- Personnel security
- Procedural (business process) security

Some Pre-HIPAA Examples of Litigation Based on Security Breach

- **Medlantic Healthcare Group:** Plaintiff sued hospital for lack of adequate security measures in protecting patient medical records when a part-time, unauthorized employee accessed and discussed with plaintiff's co-workers the plaintiff's HIV status. The hospital was held liable for $250,000, due in large part to lax security, including the inability of the medical records software used by the hospital to trace and identify who had accessed the records. Doe v. Medlantic Healthcare Group Inc., No. 97-CA3889 (D.C.Super.Ct. 11/30/99).

Some Pre-HIPAA Examples of Litigation Based on Security Breach

- **University of Montana:** Hundreds of pages of detailed psychological records concerning visits and diagnoses of at least 62 children and teenagers were accidentally posted on the University of Montana web site for 8 days. Results of psychological tests, names, birthdays, and home addresses were disclosed.

Some Pre-HIPAA Examples of Litigation Based on Security Breach

- **Eli Lilly and Co.** inadvertently revealed over 600 patient e-mail addresses when it sent a collective message to every individual registered to received reminders about taking Prozac. Although in the past, emails had been addressed to individuals, the email announcing the end of the reminder service was inadvertently addressed to all of the participants. The incident prompted the FTC to file a complaint against Lilly alleging the disclosure constituted an unfair or deceptive act under federal law. As part of its settlement with the FTC and attorneys general from 8 states, Lilly agreed to increase existing security and create an internal program to prevent future privacy violations.

Another Way The First High-Stakes HIPAA Case Might Happen

- Failure to Follow One's Own Privacy Policies and Procedures

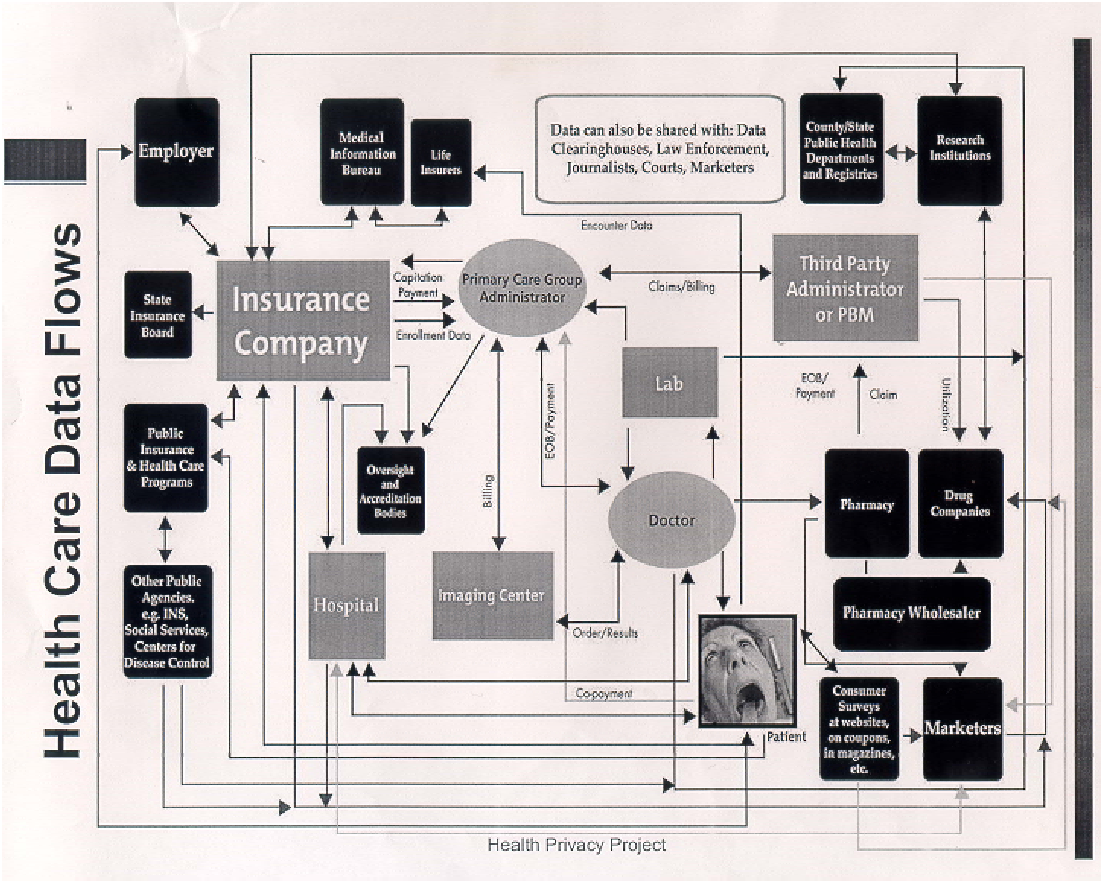
The Existing HIPAA Requirement

- HIPAA requires covered entities to adopt policies and procedures governing the protection of patient privacy.
- HIPAA also requires that notice be given to patients informing them of the covered entity's privacy policies and the patient's right to request restrictions as to use and disclosure of their PHI.

How Plaintiffs' Lawyers Might Use Non-Compliance or Breach of One's Own Privacy Policy As Basis For Lawsuit

- Likely to connect a covered entity's violation of its own policy with state law claims for:
  - negligence
  - breach of contract
  - misrepresentation

How and Where This Type of Violation Might Occur: anywhere your privacy policy touches any of these data flows



Some Pre-HIPAA Examples of Claims/Litigation

Based on Failure to Follow One's Own Privacy Policies and Procedures

- **Aetna --** Health insurance claim forms from Aetna, the nation's largest health insurer, blew out of a truck on the way to a recycling center and scattered on I-84 in East Hartford during the evening rush hour. The forms contained names and personal health information of patients. Aetna quickly dispatched employees to gather up all the forms. The forms should have been shredded under company policy, but were not (The Hartford Courant, May 14, 1999).

Some Pre-HIPAA Examples of Claims/Litigation

Based on Failure to Follow One's Own Privacy Policies and Procedures

- **Arkansas Dept. of Human Services (DHS) --** Confidential Medicaid records were disclosed during the sale of surplus equipment by the Arkansas DHS twice in 6 months. In October 2001, the state stopped the sale of DHS's surplus computer storage drives when it was discovered that Medicaid records that were supposed to be erased pursuant to DHS policy were still on the computers. In April 2002, a man who bought a file cabinet from DHS found the files of Medicaid clients still in one of the cabinet's drawers, in violation of the DHS's document destruction policy

Some Pre-HIPAA Examples of Claims/Litigation

Based on Failure to Follow One's Own Privacy Policies and Procedures

- **Eli Lilly and Co.** was sued by the FTC over its failure to honor its privacy policy, a failure which the FTC asserted constituted a deceptive trade practice. According to the FTC, Lilly's website privacy statement was false and misleading because it advised participants that their privacy was "respected" by Lilly and that Lilly believed privacy was "important" to its guests. The FTC alleged that the mistaken e-mail transmission and the absence of trained personnel made the privacy and security statements false and misleading.

The Third Way The First High-Stakes HIPAA Case Might Occur

- Medical Data Abuses or Breaches by Business Associates

The Existing HIPAA Requirement

What is a Business Associate?

- A "business associate means, with respect to a covered entity, a person who:

  (i) On behalf of such covered entity . . . performs, or assists in the performance of:

  > (A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or
  >
  > (B) Any other function or activity regulated by this subchapter; or

  (ii) Provides . . . legal, actuarial, accounting, consulting, data aggregation . . . management, administrative, accreditation, or financial services to or for such covered entity . . . where the provision of the service involves the disclosure of individually identifiable health information from such covered entity . . . or from another business associate of such covered entity or arrangement, to the person."

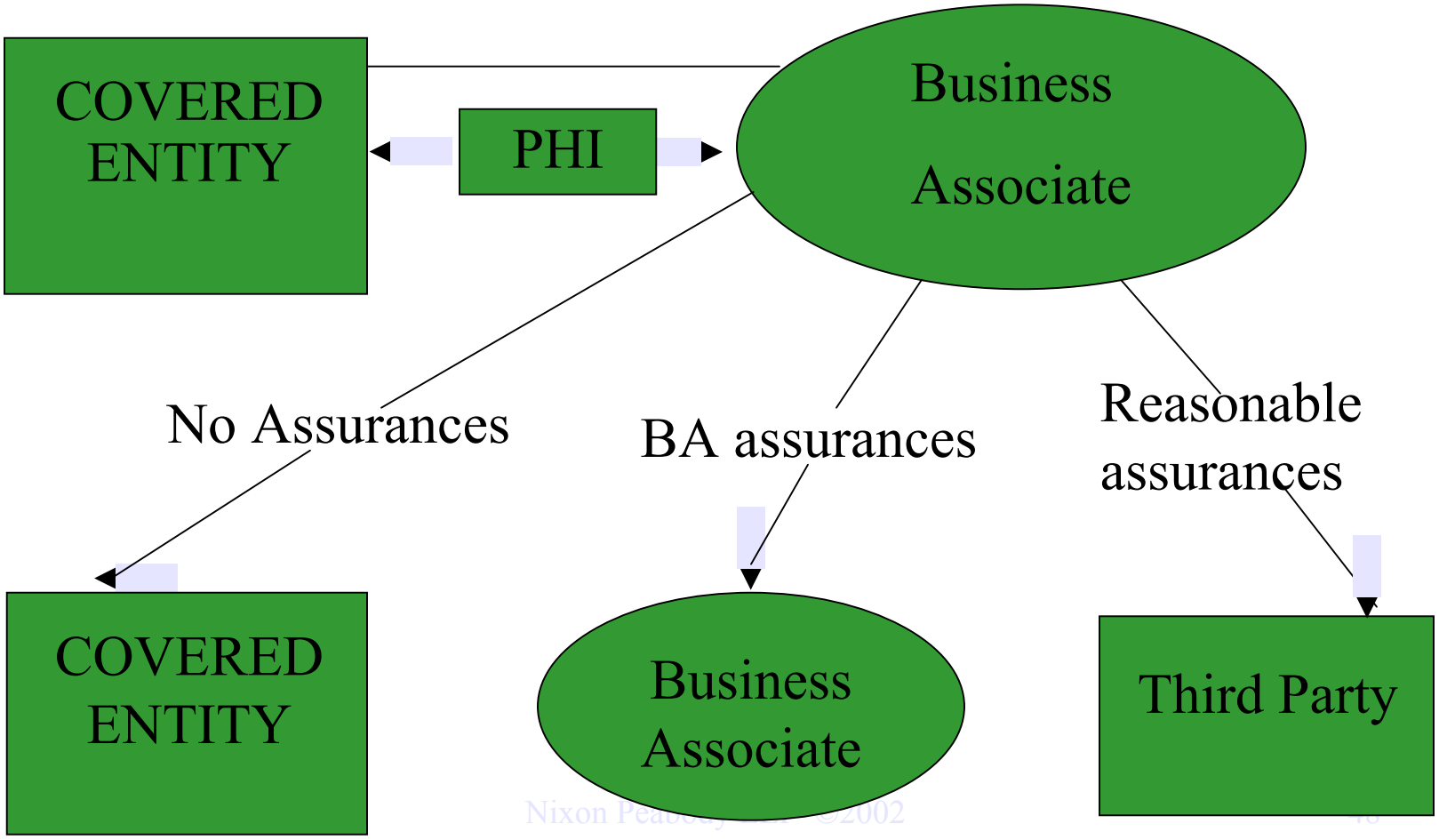
Legal Liability for the Activities of One's Business Associates

- **Covered entities** -- to an extent, you are your brother's keeper
- Must obtain satisfactory assurances that the B.A. will appropriately safeguard the information
- No automatic liability for violation by B.A., but covered entity can't avoid responsibility by intentionally ignoring problems with B.A.

How Plaintiffs' Lawyers Might Use The Satisfactory Assurance Requirement As Basis For Lawsuit

- Again, in connection with state law claims by patients for wrongful disclosure of PHI
- Plaintiffs' lawyers might be expected to argue that HIPAA requires covered entities to exercise due diligence in scrutinizing its B.A.'s security practices

How and Where Business Associate Disclosure Violations Might Occur:



Some Pre-HIPAA Examples of Claims/Litigation

Based on Activities of B.A. Type Entities/Persons

- Unauthorized, unprivileged disclosure of PHI obtained by counsel for a hospital, despite the fact that disclosure was made to counsel who represented the hospital in a proceeding that required knowledge. Biddle v. Warren Gen. Hospital, 715 N.E.2d 518 (OH. 1999).

- A medical student in Colorado sold the medical records of patients to malpractice lawyers (1997).

Some Pre-HIPAA Examples of Claims/Litigation

Based on Activities of B.A. Type Entities/Persons

- **Weld v. CVS** --Alleged wrongful disclosure of medical information by drugstore chain CVS to direct-marketing company in connection with patient-compliance program. CVS and Elensys Care Services Inc. agreed to send refill reminders and drug advertisements to CVS pharmacy customers. The mailings were sent on CVS letterhead but were paid for by the drug manufacturers whose drugs were advertised. This litigation is still pending. Weld v. CVS Pharmacy, Inc., C.A. No. 98-0897 (Mass. Super.Ct., Suffolk Co. 1998) http://www.masslaw.com/masup/1007501.htm.

Some Pre-HIPAA Examples of Claims/Litigation

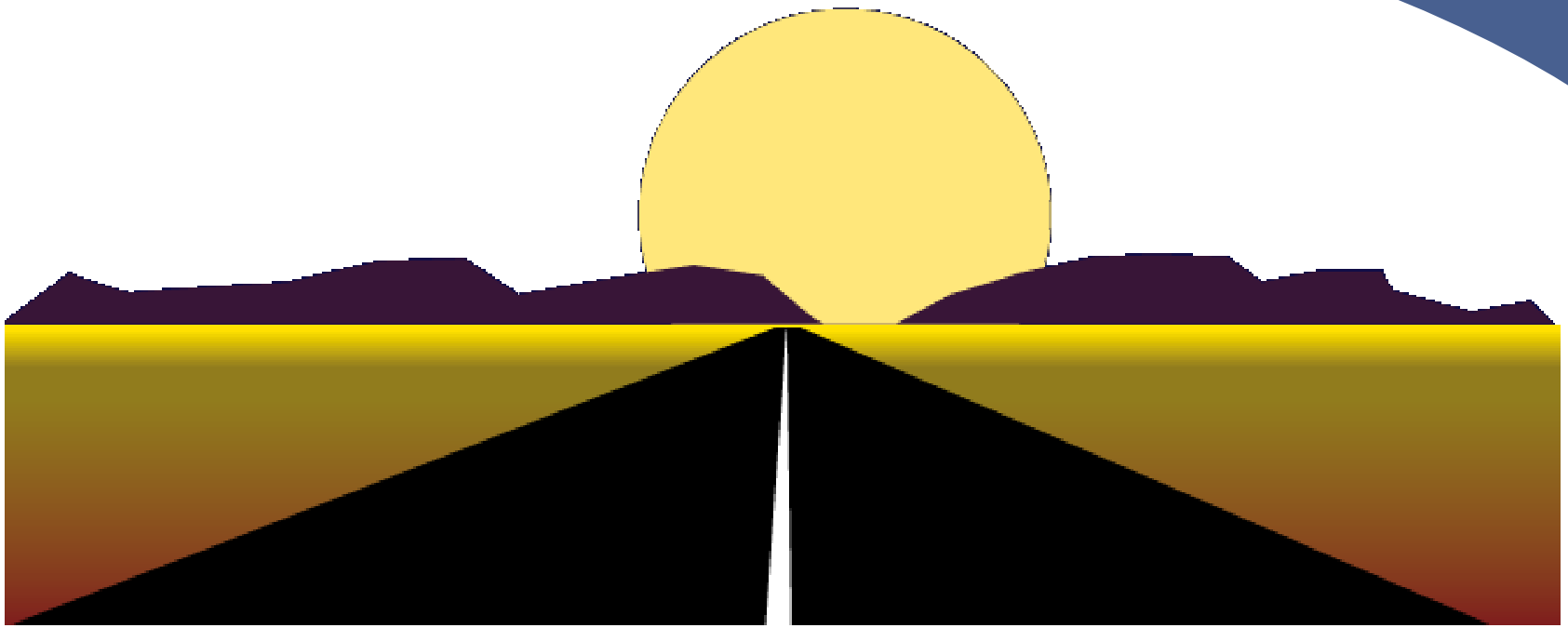
Based on Activities of B.A. Type Entities/Persons

- **Examples from outside the medical context (financial context)**
- **NationsBank** was forced to pay more than $6.5 million to settle allegations that it provided its subsidiary NationsSecurities with customer names, financial statements, and account balances to help the company sell closed-end bond funds to bank customers as their certificates of deposits matured.
- **Bank of America** was sued in a class action for selling unauthorized consumer credit reports to entities that were unaffiliated with the company in alleged violation of Fair

III. How To Minimize the Risk of Future HIPAA Litigation

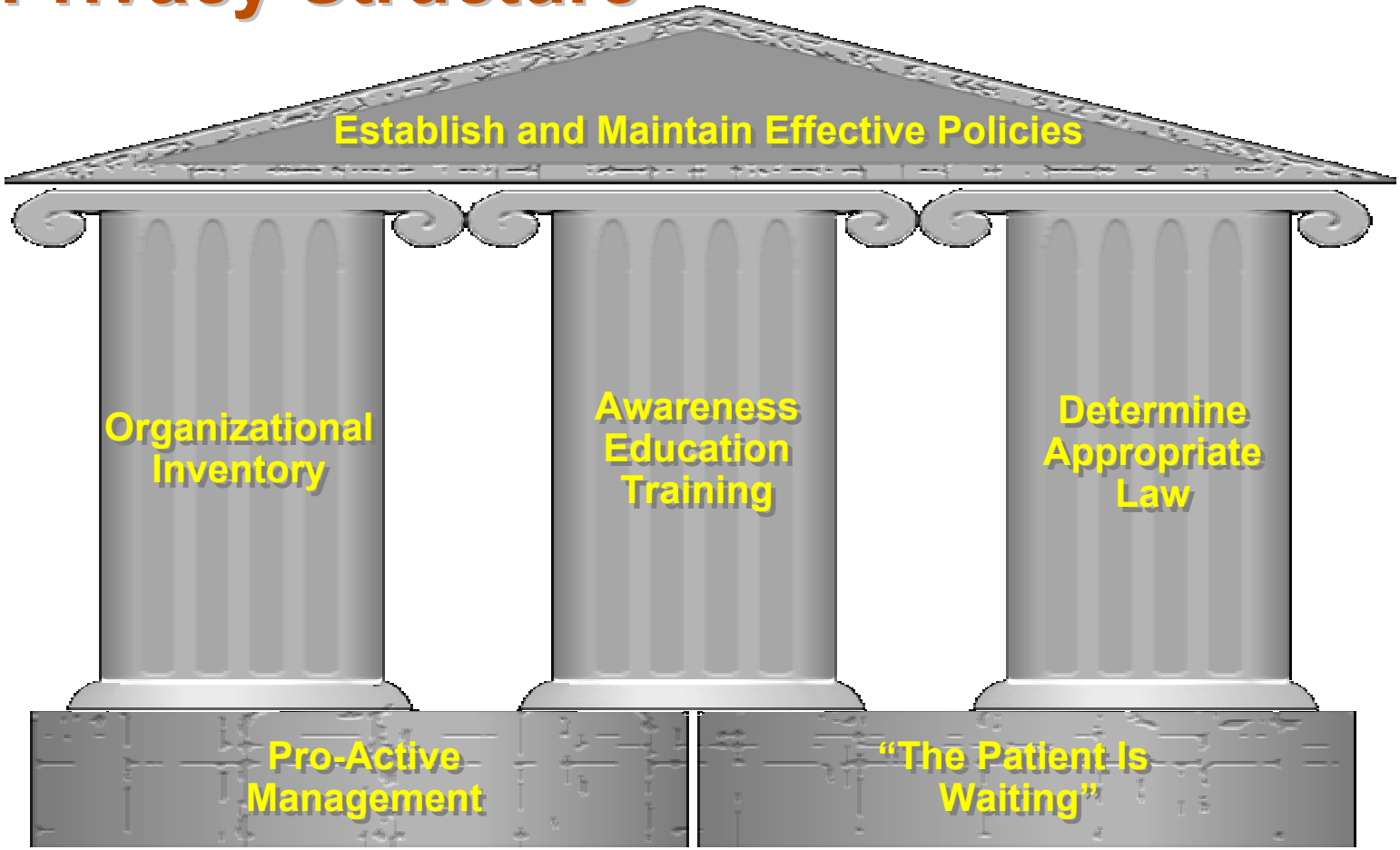
(a.k.a. How to Reduce Your Chances Of Becoming The First HIPAA Litigation Posterchild)

Think Differently About HIPAA and the Medical Privacy Function



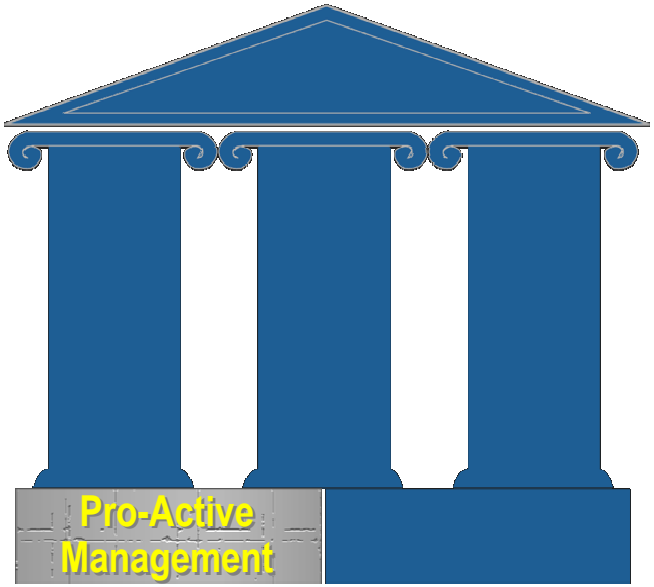
Looking Beyond Obstacles, We Can Successfully Navigate and Improve the Future Landscape

Succeed by Building a Strong Privacy Structure



Pro-Active Management

- Active – Not Reactive or Passive
- Anticipating Change, Not Responding to It

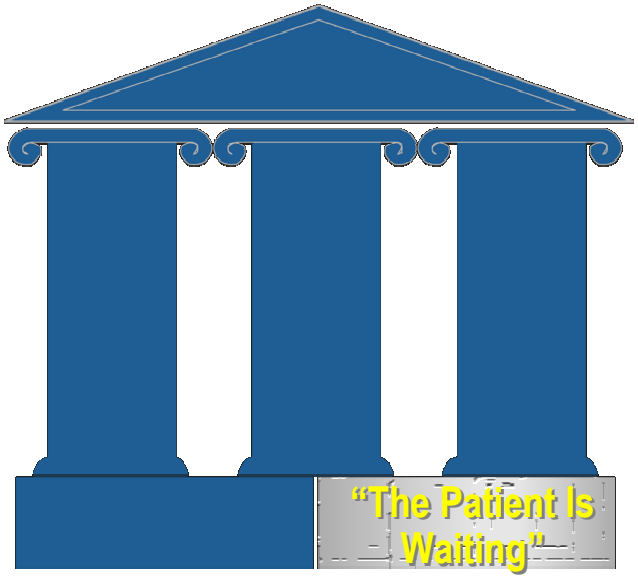


"Privacy is to the information age what environment is to the industrial age: something that needs to be attended to on the front end."

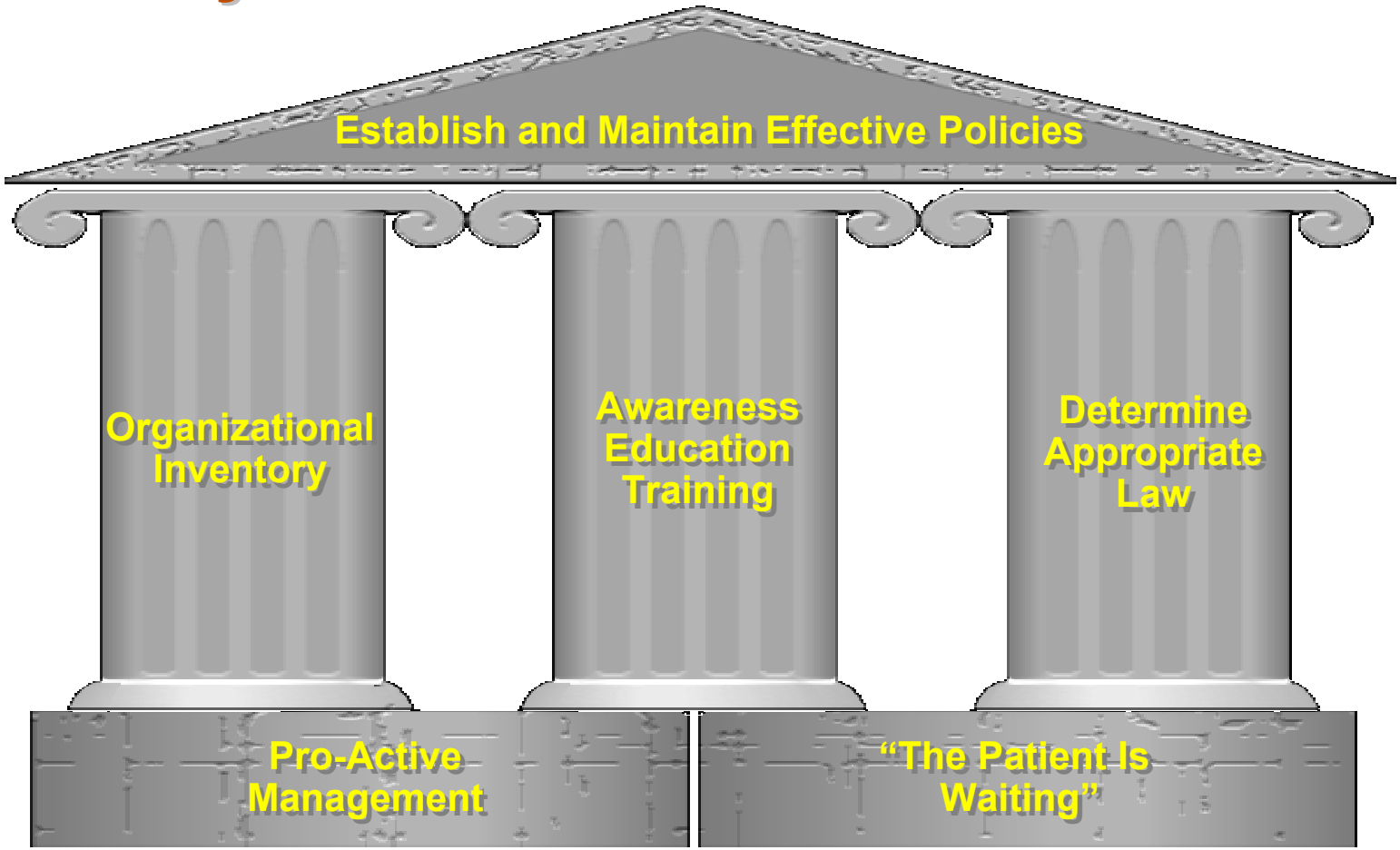
– Diedre Mulligan

Focus on the Patient

- Concerns of Patients, Consumers, and Employees
- Ask Questions from Their Perspective



Succeed by Building a Strong Privacy Structure

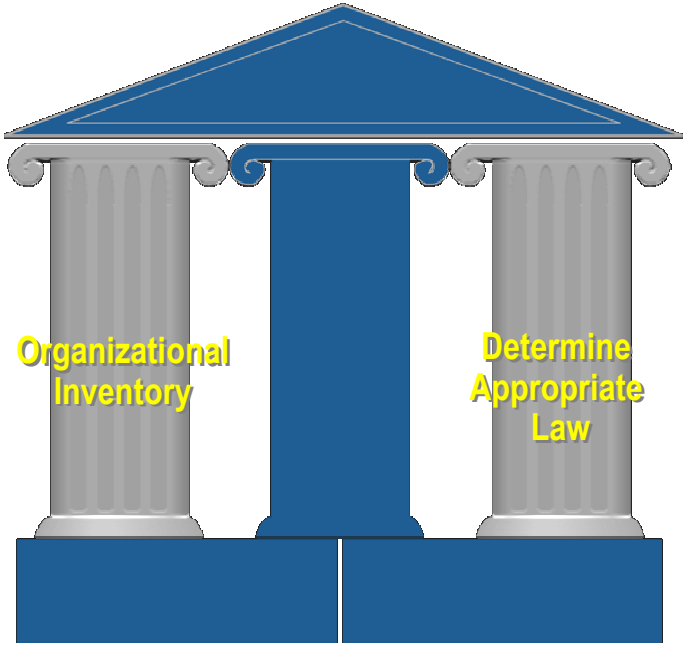


Two Fundamental Problems

- **Medical Function Diversity**
- **Regulatory Diversity**

Solutions

- Take a Good Inventory and Build Communication Bridges in the Organization



Organizational Inventory

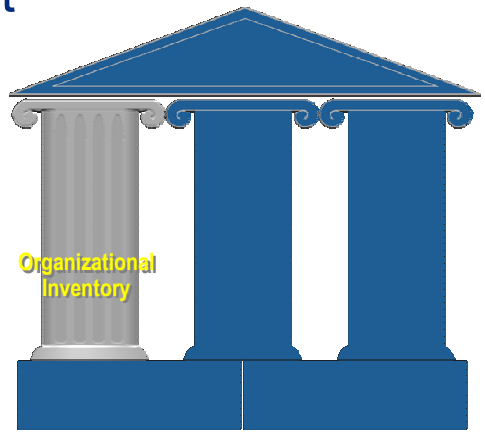
Careful Inventory of Many Parts of Organization

Obvious Areas

- Clinical Trials
- Adverse Event Reporting
- Employer Resources

Emerging Areas

- Disease Management Programs
- Interactive Internet Websites
- Customer Service Phone Lines
- Indigent Drug Access Programs
- Employee Benefit Plans
- Genetic Research

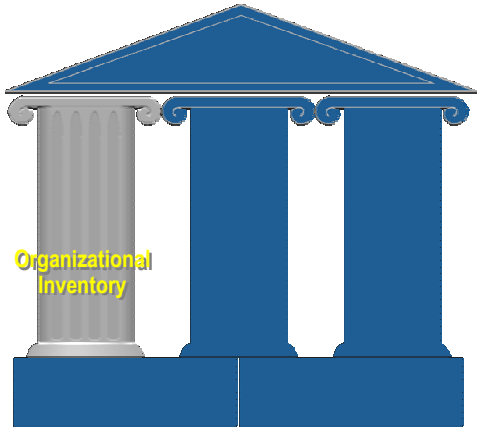


Organizational Inventory

Key Question:

Do We Handle Personally Identifiable Information As Part of this Business Function?

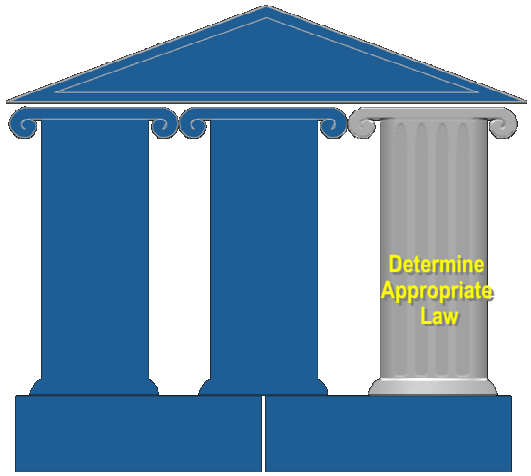
If yes, apply company policy



Determine Appropriate Law

Regulatory Diversity

- Determine appropriate law
- HIPAA is a floor, but not a ceiling



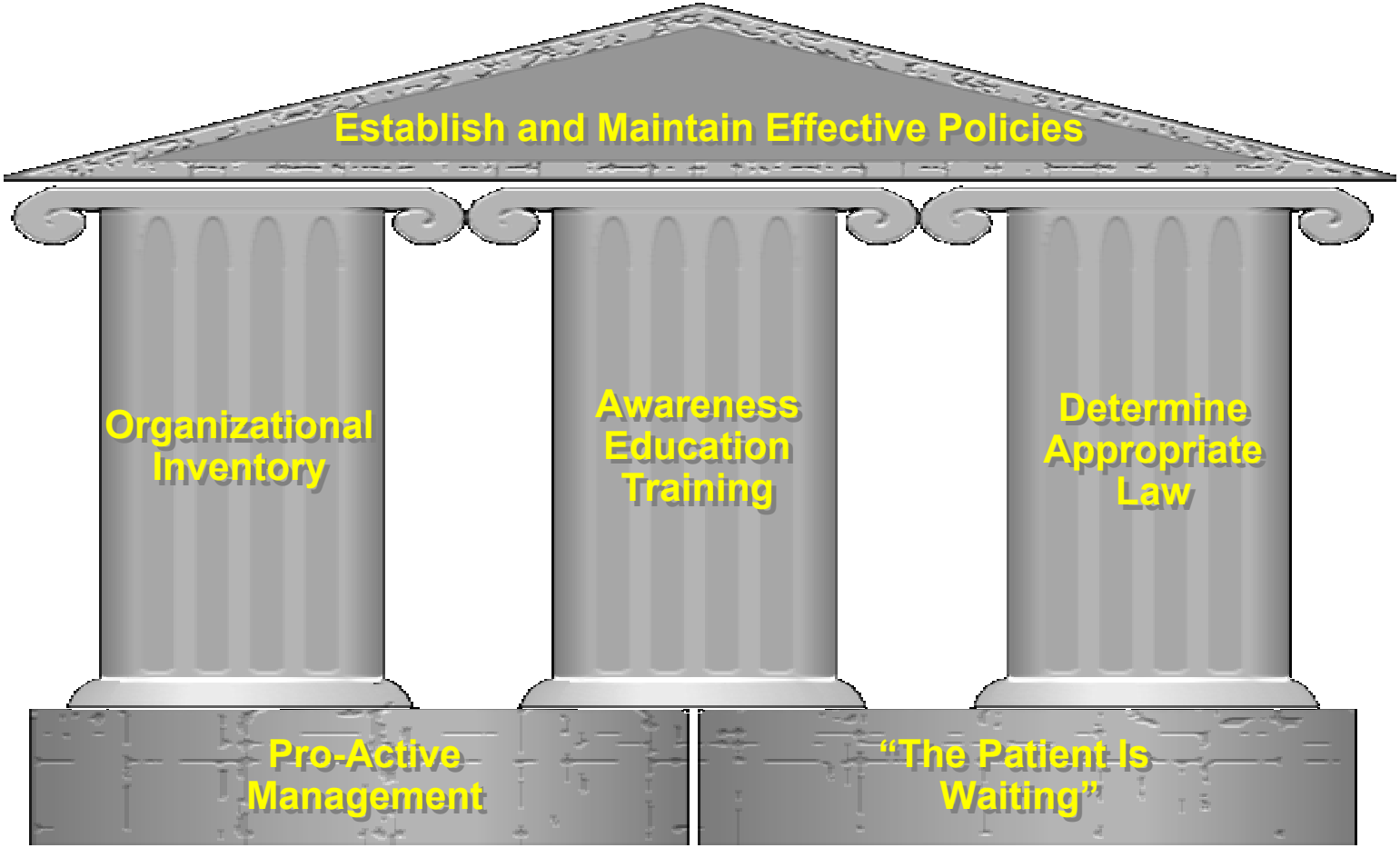
Awareness, Education, and Training

- Consciousness Raising
  - Use Employee Communication Tools
- Focus on Individual
  - Importance to Me and My Business Objectives
- Senior Management Support

Establish and Maintain Effective Policies

- Shape the Future
- Balancing of Privacy Concerns

Think Differently



How to Reach Us

- Leigh-Ann Patterson 617.345.1258
  lpatterson@nixonpeabody.com
- Ray Gustini 202.585.8725
  rgustini@nixonpeabody.com
- Sal Colletti 212.573.7596
  Sal.Colletti@Pfizer.com