

# What Works and What Doesn't:

Lessons from:

**HIPAA, GLBA, SOX**

**Margret Amatayakul,**

MBA, RHIA, CHPS, CPHIT, CPEHR, FHIMSS

Margret\A Consulting, LLC

# Margret Amatayakul

## Margret\A Consulting, LLC

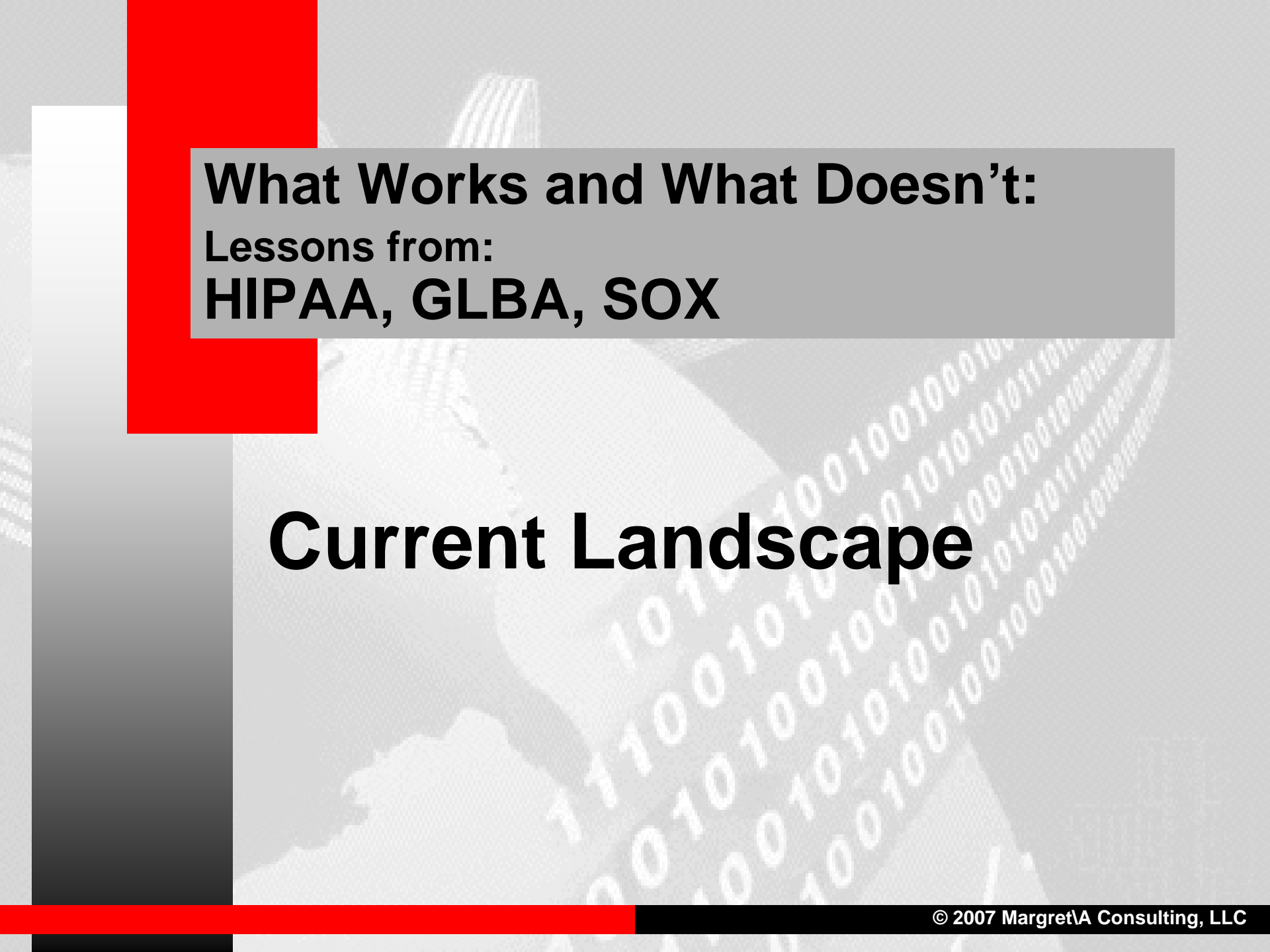
*Strategies for the digital future of health information*

- Independent consultant focusing on EHR, HIE, and associated standards and regulations
- Adjunct faculty, College of St. Scholastica, Masters in Health Informatics
- Former positions with CPRI, AHIMA, University of Illinois, Eye & Ear Infirmary
- Active participant in standards development, HIMSS BOD
- Speaker and author
- Co-founder and board of examiners, **Health IT Certification, LLC**

- Strategic HIT planning
- EHR migration path
- Compliance assessments
- Work flow redesign
- Project management oversight
- ROI/benefits realization
- Training and education
- Vendor selection
- Product/market analysis

# Agenda

- **Current Landscape**
- **Lessons Learned**
- **Need for Data Stewardship**

The background features a grayscale image of a hand holding a pen, with binary code (0s and 1s) overlaid in a perspective view. A solid red vertical bar is on the left side, and a red horizontal bar is at the bottom.

**What Works and What Doesn't:**  
Lessons from:  
**HIPAA, GLBA, SOX**

**Current Landscape**

# Current Landscape: The Good, The Bad, The Ugly

**Increasing  
Competition**

**R & D  
Demands**

**Quality &  
Performance**

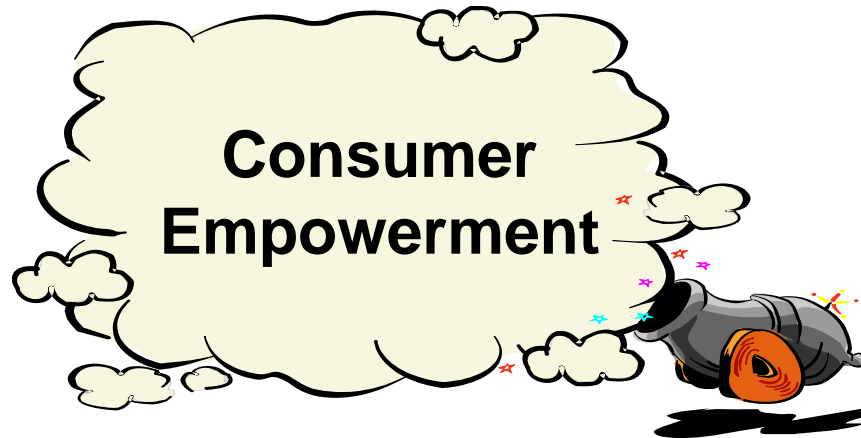
**Economy  
(Reimbursement)**

**Automated  
Data Collection**

**Internet  
Literacy**

**Data  
Mining**

**Information  
Exchange**



# Is Anything Private Anymore?

- **Google Street View** (online mapping service, has been used by employers to monitor employee smoking)
- **MySpace, Facebook** (social networking sites)
- **Fast Lane** (toll booth cameras, often used by divorce attorneys as well as toll authorities)
- **Discount cards** (save you money while collecting buying patterns)
- **Huge databases** (e.g., telephone call records, prescriptions filled that can be used to target marketing)



# HIPAA – GLBA – SOX

- **Health Insurance Portability and Accountability Act of 1996 (HIPAA) Administrative Simplification**
  - Promotes “efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information”
- **Financial Modernization Act of 1999 (a.k.a., Gramm-Leach-Bliley Act) [GLBA]**
  - “Insure the security and confidentiality of customer records and information; protect against ... threats or hazards to security or integrity of such records; protect against unauthorized access to or use of ... that could result in substantial harm or inconvenience to any customer”
  - In 2003, member agencies of Federal Financial Institutions Examination Council issued new guidance that expands GLBA to protect all information assets, not just customer information

## ■ Sarbanes-Oxley Act of 2002 (SOX)

- Founded on GLBA and HIPAA statutory standards
- Formalized by Sarbanes-Oxley disclosure requirements for publicly traded companies
- Emphasizes management's responsibility “for establishing and maintaining an adequate internal control structure and procedures for financial reporting”
- Reporting obligations cover more than GAAP, extending to material operational issues
- “A secure information infrastructure is central to many companies' operational capabilities”
- Observation: Many healthcare organizations are publicly traded; and boards and executives in non-profits are taking notice of Sarbanes-Oxley as well



# Common Privacy Areas

## GLBA

- Clear disclosure of privacy policy re: sharing of non-public personal information with both affiliates and third parties
- Requires “opt-out” of sharing of non-public personal information with nonaffiliated third parties subject to certain limitations
- Allows for flexibility to prescribe exceptions
- Remedies for violation
- Does not modify, limit, or supersede operation of the Fair Credit Reporting Act

## HIPAA

- Notice of Privacy Practices
  - Covered entities
  - Business associates and agents
- Right to *request* restrictions
- Variation between payers, CHs, and providers
- Remedies for violation
- Right to access, amend, and accounting for disclosures

# Common Security Areas

## GLBA

- **Involve board of directors**
- ★
- **Assess risk**
- **Design safeguards program\***
- **Implement security controls**
- **Train employees**
- **Oversee service providers**
- **Security testing**
- **Monitor and adjust program**
- **Report to board of directors**
- **Consumer education and assistance**

\*Written program

★ Not addressed

## HIPAA (Less process oriented)

- ★
- **Assign security responsibility**
- **Risk analysis and management**
- **Implement security controls**
- **Train workforce**
- **Business associate contracts**
- **Review and modify**
- ★
- ★
- **Documentation**

# Importance of Risk Analysis

## GLBA

- Identify reasonably foreseeable internal and external **threats** that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or information systems
- Assess likelihood and potential damage of these threats, considering **sensitivity** of customer information
- Assess sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks

## HIPAA

- In deciding which security measures to use, a covered entity must take into account:
  - Size, complexity, and capabilities
  - Technical infrastructure, hardware, and software security capabilities
  - Costs of security measures
  - Probability and criticality of potential risks to ePHI
- “Cost is not meant to free covered entities from the responsibility to implement adequate security measures”

# HIPAA Statistics

## PRIVACY

### ■ By issue

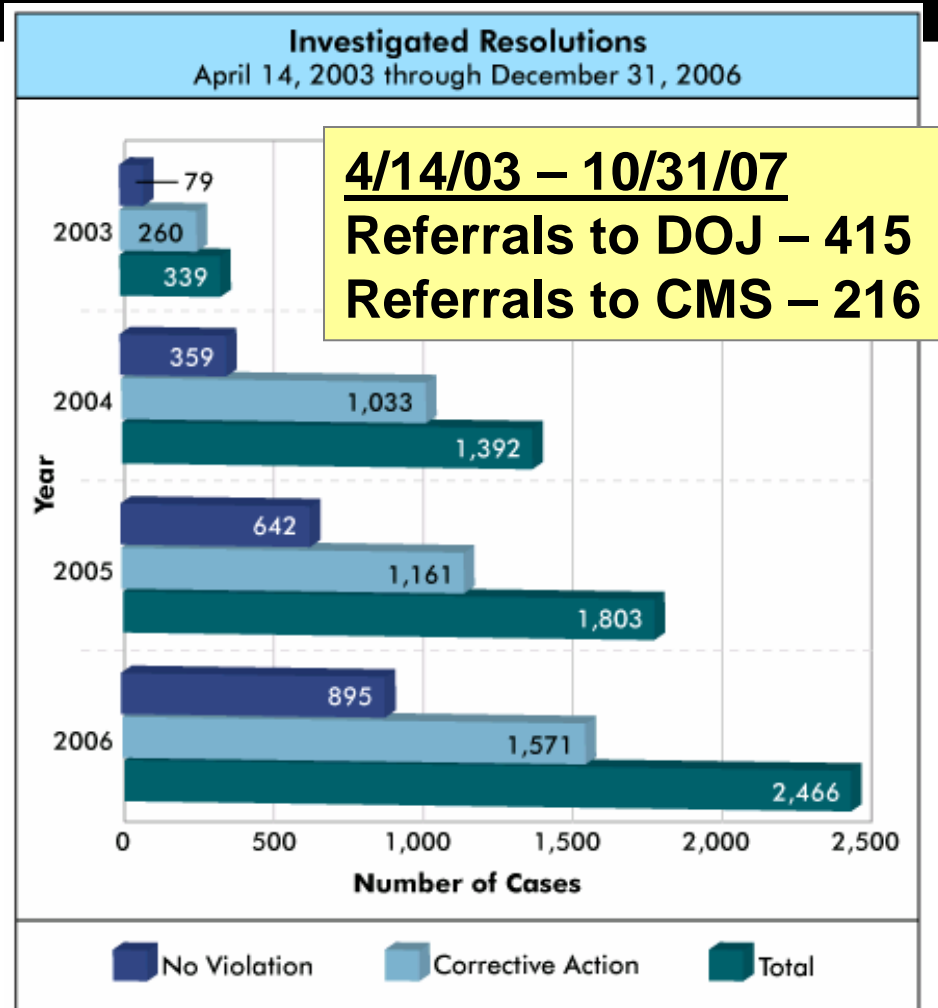
- Impermissible U&D
- Lack of safeguards
- Lack of access to PHI
- U&D not minimum necessary
- No/invalid authorization

### ■ By covered entity

- Private practices
- General hospitals
- Outpatient facilities
- Health plans
- Pharmacies

## SECURITY

- Information access management
- Security awareness & training
- Access control
- Workstation use
- Device and media controls

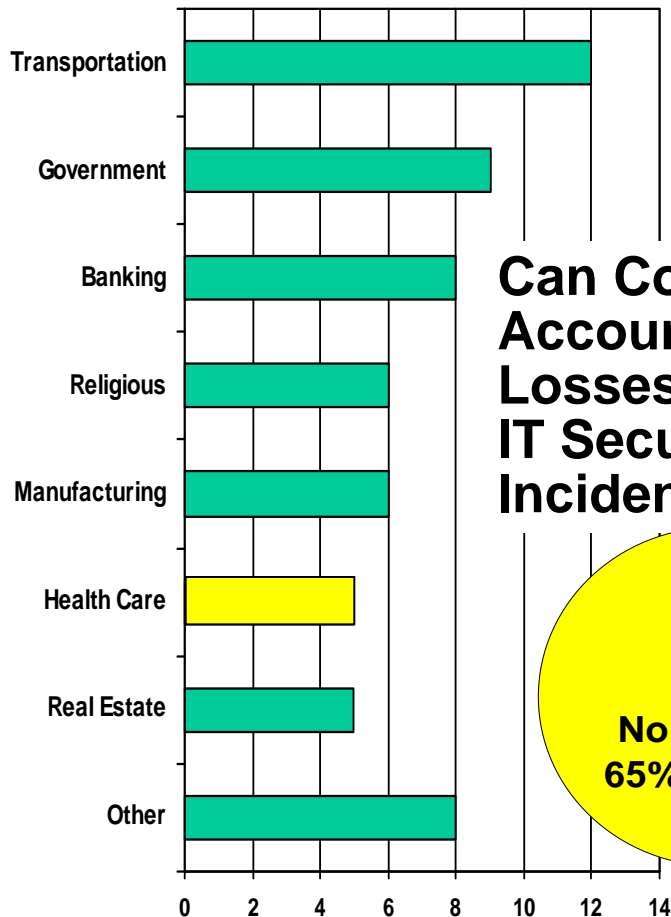


[www.hhs.gov/ocr/privacy/enforcement/numbersglance.html](http://www.hhs.gov/ocr/privacy/enforcement/numbersglance.html)

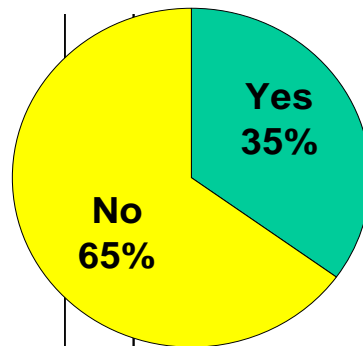
**4/20/05 – 10/31/07**  
**Security complaints – 370**  
**Ongoing investigation – 140**  
**Audits initiated**

# Some General Security Statistics

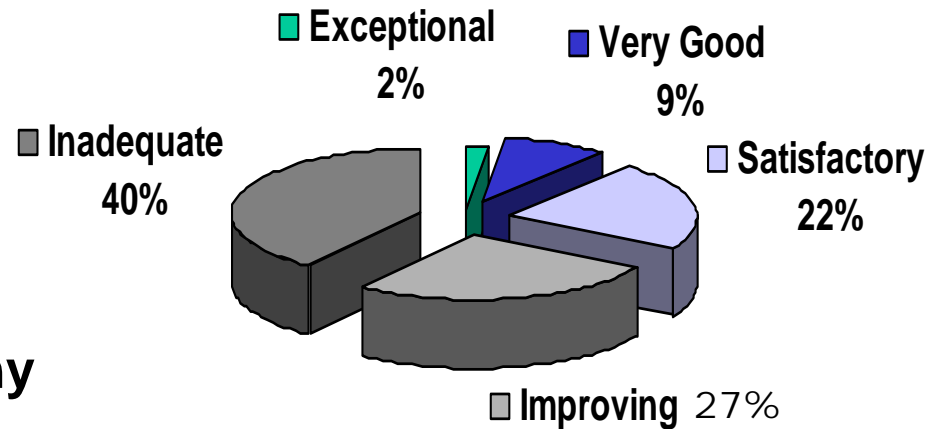
## Security Budget as a Portion of IT Budget by Industry Type



## Can Company Account for Losses from IT Security Incidents?



## Administrative Resources

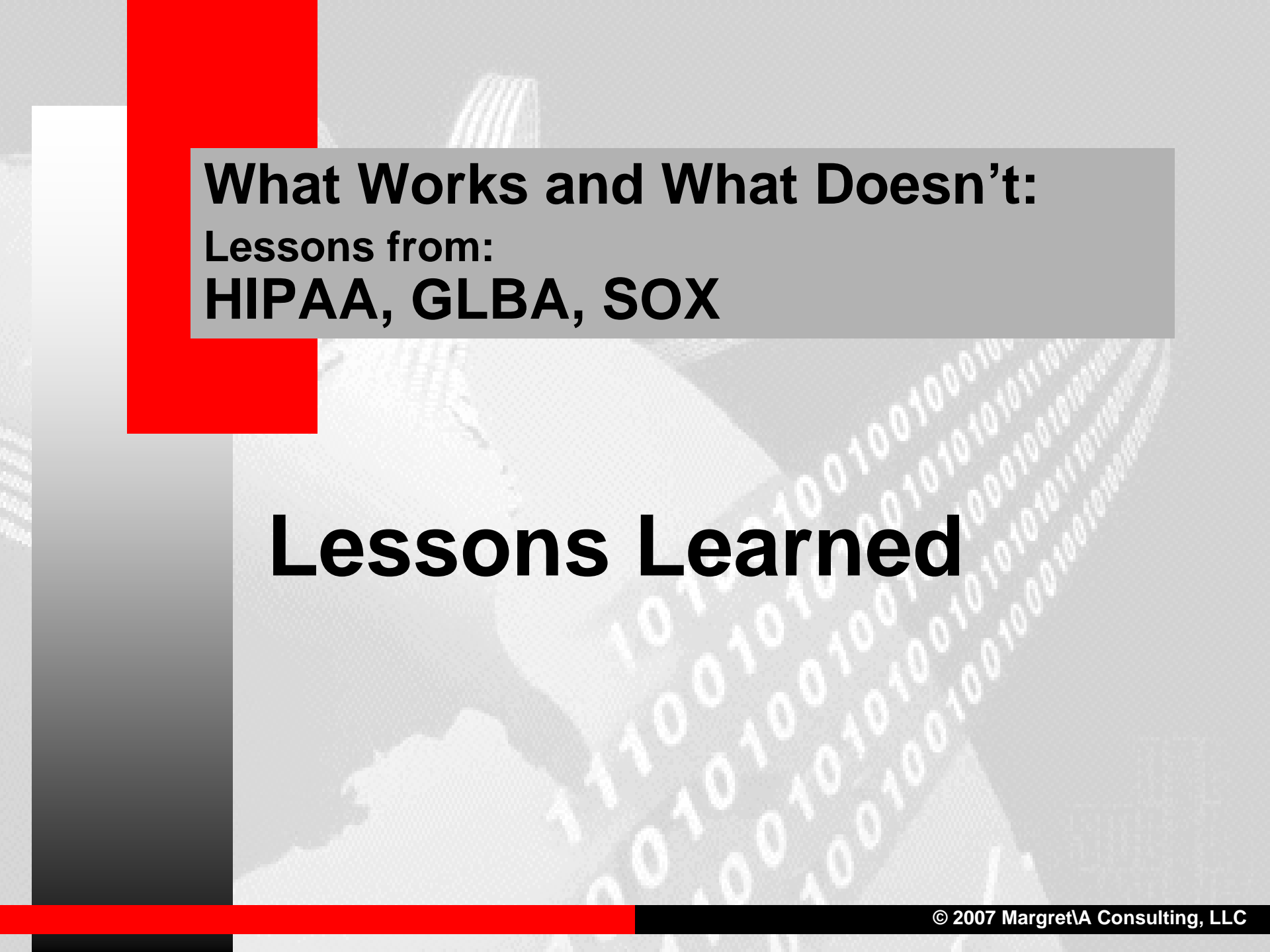


## Network World:

	Median % of IT Budget	Range of Spending
2005	3.9%	5 – 7%
2006	4.7%	5 – 10%
2007	5.9%	5 – 12%

## Security Incidents:

2/3 = Administrative errors, insider abuse, stolen equipment  
 1/3 = Hackers

The background features a grayscale image of a hand holding a pen, with binary code (0s and 1s) overlaid. A prominent red vertical bar is on the left side of the slide.

**What Works and What Doesn't:  
Lessons from:  
HIPAA, GLBA, SOX**

**Lessons Learned**

# Lessons Learned: Plain Language

## ■ GLBA Privacy Notices:

- Too lengthy
- Dense in content
- Complex language
- Consumers neither read nor understood

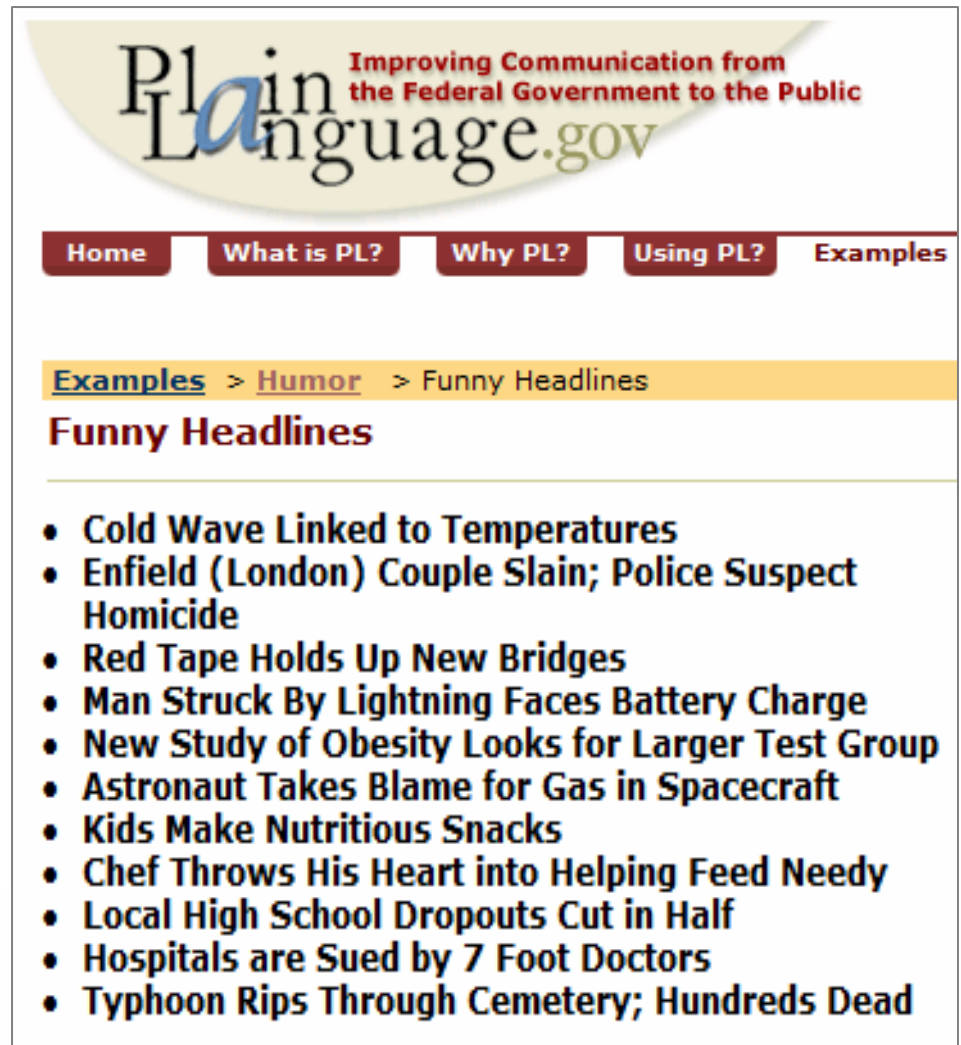
## ■ Response:

- Multi-Agency Form Development Project

### **S.E.C. Sends Lawyers Back to English Class**

*Oct. 9, 2007 - Portfolio.com - by Megan Barnett*

The Securities and Exchange Commission has completed its initial review of how 350 public companies have complied with the compensation disclosure requirements that went into effect in November 2006. The S.E.C. wanted companies to disclose more detailed information on how and what it pays its officers, and it wanted it in plain English.



The screenshot shows the Plain Language.gov website. The header includes the logo "Plain Language.gov" with the tagline "Improving Communication from the Federal Government to the Public". Below the logo is a navigation menu with buttons for "Home", "What is PL?", "Why PL?", "Using PL?", and "Examples". The "Examples" button is highlighted, and a breadcrumb trail shows "Examples > Humor > Funny Headlines". The main content area is titled "Funny Headlines" and lists ten humorous headlines:

- Cold Wave Linked to Temperatures
- Enfield (London) Couple Slain; Police Suspect Homicide
- Red Tape Holds Up New Bridges
- Man Struck By Lightning Faces Battery Charge
- New Study of Obesity Looks for Larger Test Group
- Astronaut Takes Blame for Gas in Spacecraft
- Kids Make Nutritious Snacks
- Chef Throws His Heart into Helping Feed Needy
- Local High School Dropouts Cut in Half
- Hospitals are Sued by 7 Foot Doctors
- Typhoon Rips Through Cemetery; Hundreds Dead



# Could the healthcare industry do this?

Evolution of a Prototype Financial Privacy Notice, Kleimann Communication Group, Inc., Feb. 28, 2006

FACTS		WHAT DOES NEPTUNE BANK DO WITH YOUR PERSONAL INFORMATION?	
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.		
What?	<p>The types of personal information we collect and share depend on the product or service you have with us. This information can include:</p> <ul style="list-style-type: none"> <li>▪ social security number and income</li> <li>▪ account balances and payment history</li> <li>▪ credit history and credit scores</li> </ul> <p>When you close your account, we continue to share information about you according to our policies.</p>		
How?	All financial companies need to share customers' personal information to run their everyday business—to process transactions, maintain customer accounts, and report to credit bureaus. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons Neptune Bank chooses to share; and whether you can limit this sharing.		
Reasons we can share your personal information	Does Neptune Bank share?	Can you limit this sharing?	
For our everyday business purposes—to process your transactions, maintain your account, and report to credit bureaus	Yes	No	
For our marketing purposes—to offer our products and services to you	Yes	No	
For joint marketing with other financial companies	Yes	No	
For our affiliates' everyday business purposes—information about your transactions and experiences	Yes	No	
For our affiliates' everyday business purposes—information about your creditworthiness	Yes	Yes (Check your choices, p.3)	
For our affiliates to market to you	Yes	Yes (Check your choices, p.3)	
For nonaffiliates to market to you	Yes	Yes (Check your choices, p.3)	
Contact Us	Call 1-800-898-9698 or go to <a href="http://www.neptunebank.com/privacy">www.neptunebank.com/privacy</a>		



# **(SOX) Compliance Lessons**

(Forrester Research)

- **Costs soared well beyond expectations**
- **Technology was underutilized**
- **Regulatory guidance was insufficient and unclear; e.g., what is a “material weakness”**
- **Audits were often not top-down, not risked-based**
- **Numerous control deficiencies uncovered**
- **Financial management systems were in need of repair**

**Does this  
sound like  
results  
from  
HIPAA?**

# Opt-in/Opt-Out Lessons from the Web?

- Opt-in – requires an action or affirmation by an individual for inclusion; the default is exclusion
- Opt-out – requires an action or affirmation for exclusion; the default is inclusion
- High interest in healthcare for
  - HIE/NHIN
  - PHR
  - EHR

## Applicability to Healthcare

- More than “request for restrictions”
- You can’t do both simultaneously
- Choice frequently depends on trust
- Both have risks and benefits
  - To providers
  - To individuals

# **What Works and What Doesn't:**

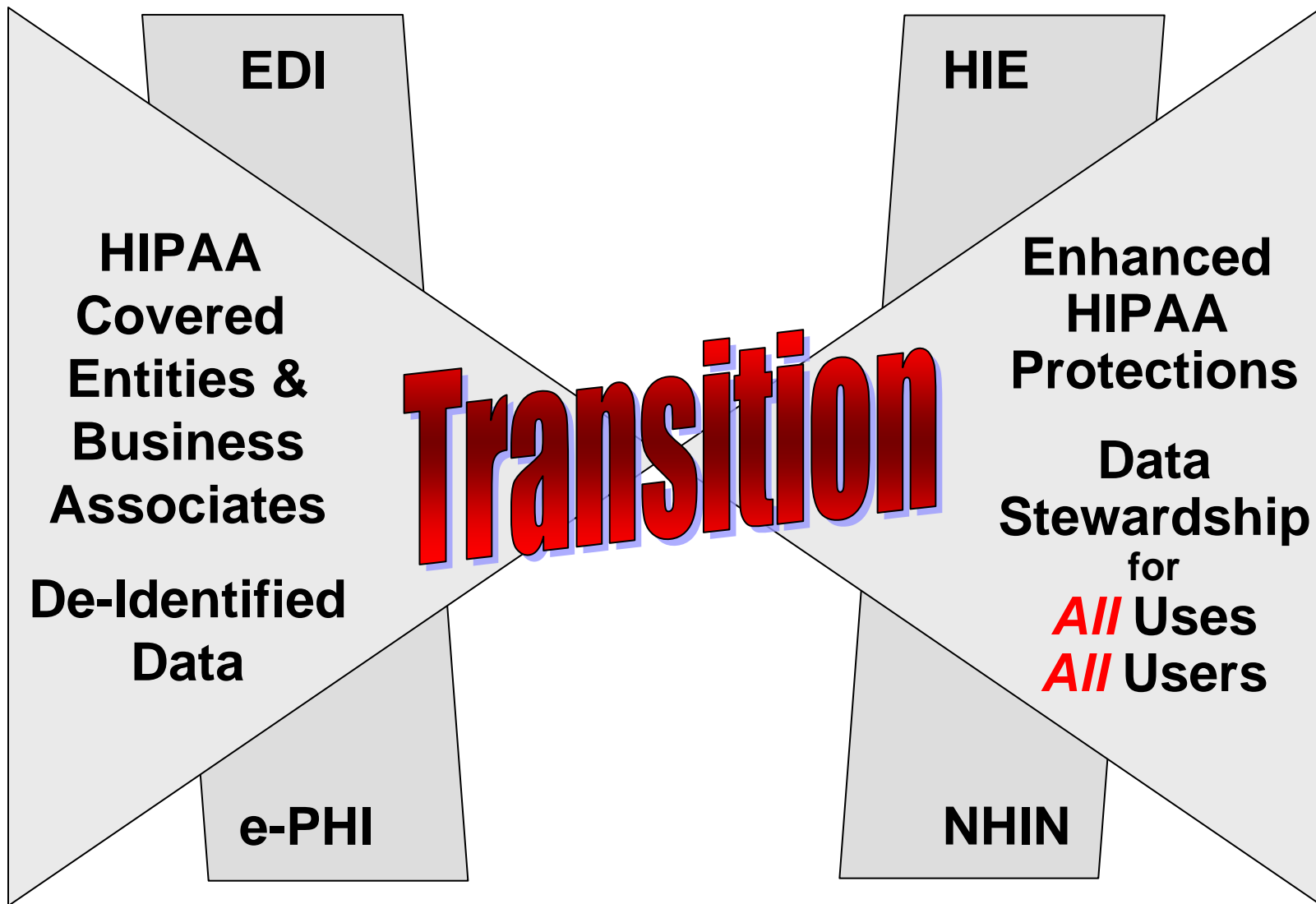
**Lessons from:**

**HIPAA, GLBA, SOX**

## **Need for Data Stewardship**

# Data Stewardship

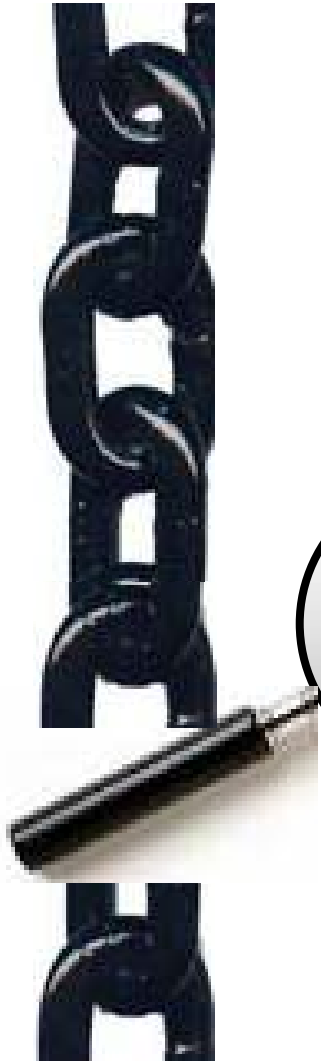
- **Stewardship . . .** Is personal responsibility for taking care of something one does not own
- **Data stewardship** (corporate) is the management of the corporation's data assets in order to improve their reusability, accessibility, and quality. Data stewardship needs are especially recognized when using data warehouses for data mining
- **Health data stewardship** (AMIA) “encompasses the responsibilities and accountabilities associated with managing, collecting, viewing, storing, sharing, disclosing, or otherwise making use of personal health information”



# Health Data Stewardship

- **Accountability/Chain of Trust**
- **Transparency**
- **Individual Participation**
- **HIPAA De-identification**
- **Security Safeguards and Controls**
- **Data Quality and Integrity**
- **Oversight of Data Uses**

# Chain of Trust



- Individual
- Covered entity
  - Treatment
  - Payment
  - Healthcare Operations
- Business associate
- Agent(s) of business associate
- Non-covered organizations
- Protected health information
- Aggregated data
- De-identified data
- Data linkage
- Data mining
- Personal health information

# Contact Information

**Margret\A Consulting, LLC**

**Schaumburg, IL 60193**

**Tel. 847-895-3386**

**Margret@Margret-A.com**

**www.Margret-A.com**