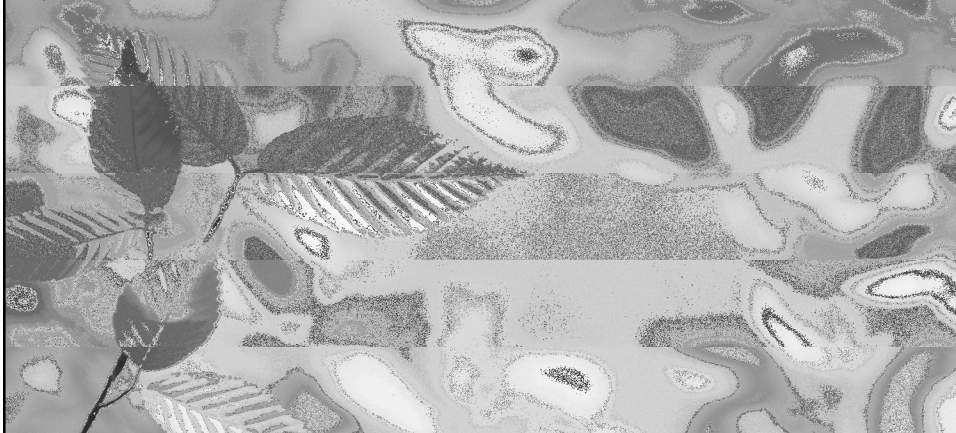



Moving Beyond HIPAA: 10 Things Healthcare Organizations Need to Know About Breach Compliance & Medical Identity Theft*

Health Care Compliance Association's Compliance Institute

April 27, 2009



*connectedthinking
PricewaterhouseCoopers

PRICEWATERHOUSECOOPERS 

Introduction

James H. Koenig, JD, CIPP

Leader
Privacy & Identity Theft Practice

james.h.koenig@us.pwc.com

610-246-4426

• For the last 3 years, Forrester has recognized PwC as tied for or the sole leading privacy and security practice, noting our integrated approach to privacy, security and identity theft prevention as a leading factor

• In 2006 and 2007, ComputerWorld, recognized PwC as tied for the top consulting firm with a Privacy Practice
• Also, ComputerWorld recognized James Koenig as one of the top 25 privacy consultants in the World.

PricewaterhouseCoopers is ranked as the leading professional services firm providing information security and data privacy services to Global 2000 organizations. IDC, The Shifting Landscape: U.S. Information Security Services, 2003.

PricewaterhouseCoopers

Slide 2

Agenda/Contents

1. Trends & Developments in Medical Identity Theft
 2. Medical Identity Theft and Breach Notification Laws
 3. Top Ten Risk You May Not Be Adequately Addressing
 4. Five Preventative Approaches to Limiting Exposure
- Questions

Section 1. Trends & Developments in Medical Identity Theft - What is it and how can it happen?

Medical Identity Theft By the Numbers

Definition. A form of fraud where either:

- An individual's name and various personal identifiers are used by another individual to fraudulently obtain medical services and goods.
- Stolen personal identifiers are used to orchestrate broad-scale health insurance billing frauds.

Victims.

- **Fast Growth.** In 2005, 250,000 Americans were victims of medical ID theft, a 334% increase over 2001 (versus a 297% increase for all identity theft).
- **4 % Experienced Lost or Stolen Medical Records.** A Harris Poll reported that 4% (or 9 million people) indicate that they or a family member have had personal medical information either lost or stolen.
- **\$1-\$2 Billion Annual Losses from Medical Identity Theft.**
 - **3%** of overall \$30-\$60 billion identity theft
 - **2%** of overall \$30-\$60 billion health care fraud

History of Information Thefts

Medical Identity Theft is part of the evolution of information crimes.

1960 and Earlier – Cold War

1970 – Industrial Espionage

1980 – Insider Trading

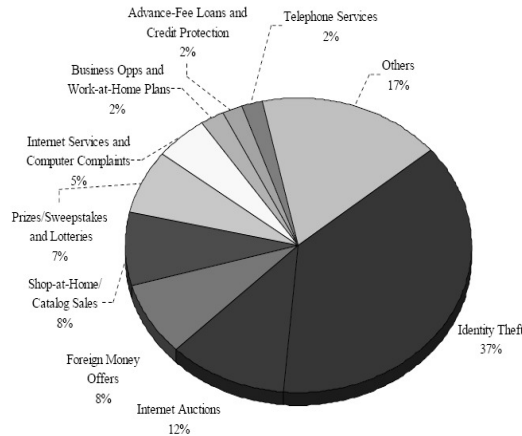
1990 – Intellectual Property

2000 – Financial Identity Theft

2009 – Medical Identity Theft

Identity Theft Overall Has Become a Major Concern

- Number one complaint to FTC
- Impacts 4.6% of US per year
- 2006 survey, companies reported ID Theft:
 - 10% globally
 - 9% in US
 - 19% in India
- \$50+ billion in losses
- 68.2% obtained off-line
- 50% conducted by employees and contractors



Impact. Higher theft risks: SSN, Driver's License Number, Credit Card Number, Health Insurance ID Number

Sources: (Javelin/BBB 1/06; Gartner 7/03; Experian-Gallup 8/05; FDIC 2/06; FTC 1/06; SMU 8/04)
PricewaterhouseCoopers

Slide 7

Identity Theft – A Closer Look

Where? Almost all studies agree that the top states in terms of victims per capita are: New York, California, Nevada, Arizona, Washington, and Texas. The Id Analytics study 2007 includes Hawaii, Illinois, Oregon, and Michigan. The FTC 2006 report includes Florida, Georgia and Colorado.

Types of Identity Theft. (2007 ID Analytics)

True-name identity theft. Identity theft victimizes an actual consumer accounts for 10-15% of all identity fraud.

- **Example** - Using someone else's benefits - someone you know versus someone with a common name
 - Hijacking Accounts
 - Access to Benefits, Medical Identity Theft (services)
- **Imposter relationship to victim:** In 2004, 43% knew their imposter, of which 14% said that it was an employee of a business who had their information

Synthetic identity fraud. Identity fraud using identities fabricated from real and false data accounts for 85-90% percent of all identity fraud.

- **Example** - Use of benefit information to build profile to exploit elsewhere.

PricewaterhouseCoopers

Slide 8

Profile of Medical Identity Thieves and Means to Monetizing

Profiles of Medical Identity Thieves

- Individual desperately needing medical care
- Health care professionals aiming to pad their income by filing fraudulent claims/diagnosis
- Organized crime rings stealing medical records and doctor billing codes

Monetizing Medical Identity Theft

- **Value of a Record.** Health records fetch \$50 to \$60 on the black market (versus \$100 for bank account records or 7 cents for stolen résumés)
- **One-Off Frauds - Friends and Family Plan.** An individual obtains identifying information of another to fraudulently obtain access to medical care/equipment.
- **Insurance Fraud.** Large-scale thefts of personal information used for insurance billing schemes. The crime can be lucrative and minimal risk.
 - **\$\$\$.** Medical records sell for as much as \$60 per name on the black market.
 - **Minimal Risk.** Financial identity theft amounts and detection thresholds are lower as are time period before awareness or scrutiny (days versus months).

PricewaterhouseCoopers

Slide 9

Medical Identity Theft Insurance Fraud Schemes

Typical Scenario. Use of stolen information to fabricate insurance claims.

- **US v. Diaz (7/08).** All-Med Billing Corp./Diaz stole the identities of physicians and forged prescriptions and other documents to support claims for durable medical equipment.
 - \$420 million in fraudulent claims submitted over six years on behalf of 85 sham equipment suppliers. Medicare paid \$148.5 million.

Clinic Takeover Scheme. Organized crime establishes a clinic, offers discounted services, collects and exploits health insurance IDs and abruptly closes.

- **US v. Dzhuga (10/07).** For nine weeks in 2003, Milpitas Medical Clinic took out ads catering to Vietnamese immigrants.
 - Promising free checkups, free transportation to clinic and gifts of nutritional supplements and Chinese medicated ointments.
 - Patients received exams from unqualified medical personnel and sent home with free gifts.
 - Staff photocopied Medicare identification cards and billed \$1.1 million in services performed by bogus diagnostic firms. Medicare paid \$909,000.

PricewaterhouseCoopers

Slide 10

Section 2. Medical Identity Theft & Data Breaches Laws - Key Things to Know

THE COST OF A BREACH: \$90 TO \$305 PER RECORD

A security breach can cost . . . anywhere between \$90 and \$305 per record. . . . The cost of a single, significant breach may run into millions or even billions of dollars [and] will vary significantly based on the public profile of the breach and the regulations that apply . . . which varies from industry to industry.

"Calculating The Cost Of A Security Breach," Forrester Research, April 10, 2007.

PricewaterhouseCoopers

Data Breaches -- A Key Board and Management Issue

Board and Management Issue. Privacy and information risk management have been elevated to the board, audit committees and senior executives as key issues given the business impacts of failure – on both long-term relationships and value.

Increased Regulator Focus on Data Protection & Breaches

- **Audits.** Federal and State regulators (including DHHS OIG) has begun auditing health care organizations for compliance and risk.
- **Enforcements.** Federal and State regulators have all been aggressively inspecting and pursuing privacy breaches and lack/failure of safeguards.
- **Damages Paid.** In the last 3 years, over \$370 million paid by companies in fines, penalties and class-actions related privacy breaches, incidents and non-compliance.
 - Recent settlement of more than \$60 million paid by a Fortune 500 company for inappropriately sharing customer information.
 - Another company set aside \$128 million related to their incident.

PricewaterhouseCoopers

Slide 12

New Laws Increasingly Driving Public Disclosures

- **Leading Brands Have Had Incidents.** Areas include vulnerable wireless networks, lost/stolen laptops/back-up tapes, marketing and fulfillment, at-home workers, call centers, web sites, vendors, HR area and more.
- **New Laws That Require Disclosures of Breaches and Data Mishandling.** New laws and guidelines in US, Japan, UK, Canada, Australia and potentially elsewhere require notices to be sent upon a data breach or mishandling of personal information. 44 states in the US passed laws in 2005-2008.
 - **Note:** Only Arkansas and California include Health Information in Law.
- **New SSN Laws.** More than half of the US states have new laws that restrict the use of Social Security Numbers as a key identifier in access controls for consumers, employees and web sites, in mailing, faxes and other marketing materials, on pay stubs.
- **Data Element Approach:** Many companies have started protecting data and approaching compliance at the data element level, not the system and application level.

Privacy Laws Overview - Health Information Technology for Economic and Clinical Health Act (HITECH Act)

Stimulus Bill. On February 17, 2009, President Obama signed the American Recovery and Reinvestment Act of 2009 ("ARRA"). Part of ARRA, HITECH Act strengthens/expands the scope of HIPAA privacy and security rules, including:

- **Penalties.** Increases penalties for violations; allows attorney general enforcements.
- **BAs.** Treats business associates as covered entities – civil/criminal penalties.
- **New PHI Federal Breach Notification Law.**
 - Requires notification within 60 days to each individual whose "unsecured" PHI is reasonably believed to have been accessed, acquired, or disclosed.
 - Business associates must notify covered entities.
 - If breach ≤ 500, notice must be provided to HHS. HHS will post on its Web site.
 - If breach ≤ 500 residents of a state, notice must be made to prominent local media.

Privacy Laws Overview - Identity Theft Red Flags Rule (A 2008 Amendment To FCRA)

Red Flags Rule – Compliance by May 1, 2009.

- Applies to financial institutions and non-FS creditors offering "covered accounts"
- **Covered Accounts are either:**
 - Consumer-related transactional accounts offered by banks, credit and debit card issuers, and other creditors (such as mortgage lenders, telecommunications companies and utilities)
 - Accounts that potentially have a "reasonably foreseeable risk of identity theft"
- **Different than data protection/ID theft prevention requirements.**
- **Identify, Assess and Implement appropriate red flag "triggers."**
The 26 specific criteria are divided among 5 categories:
 - Alerts, Notifications, or Warnings from Consumer Reporting Agencies;
 - Suspicious Documents;
 - Suspicious Personal Identifying Information (PII);
 - Unusual Use of, or Suspicious Activity Related to, the Covered Account; and
 - Notice from Customers, Victims, Law Enforcement, or Other Persons Regarding Possible Identity Theft.

PricewaterhouseCoopers

Slide 15

Privacy Laws Overview – Genetic Information Nondiscrimination Act of 2008 (GINA)

Genetic Information is defined as:

- Results of genetic tests (individual and his/her family members) that provides information about an individual's family medical history.

Key Provisions

- **Prohibits Discrimination.**
 - Employers cannot make decisions about hiring, firing, job placement, or promotion based on genetic information.
 - Group health plans cannot use genetic information for underwriting purposes or to determine premiums.
- **Restricts Acquisition.**
 - Employers and Group Health Plans may not request, require, or purchase genetic information.
- **Requires Confidentiality.**
 - Safeguards must be in place to ensure proper collection and maintenance of genetic information, as well as to protect files from unauthorized access.
GINA also limits disclosure of genetic information.

PricewaterhouseCoopers

Slide 16

Section 3. Top Ten Risk You May Not Be Adequately Addressing

PricewaterhouseCoopers

Common Vulnerabilities & Practices that Compromise SSNs & Sensitive Data

- Mobile and home-based workforce, laptops and portable devices
- Third-party vendor and outsourcing handling, transfers and lost records
- Mishandling and theft of back-up tapes
- Paper handling and dumpster diving
- Call centers and social engineering
- Collecting/using SSNs and personal information more than necessary (and not properly de-identifying and masking information)
- Improper access or broad access controls
- Unauthorized software & use of peer-to-peer networks/accidental file sharing
- One-off and other DTC mis-mailings
- Record retention and eDiscovery

PricewaterhouseCoopers

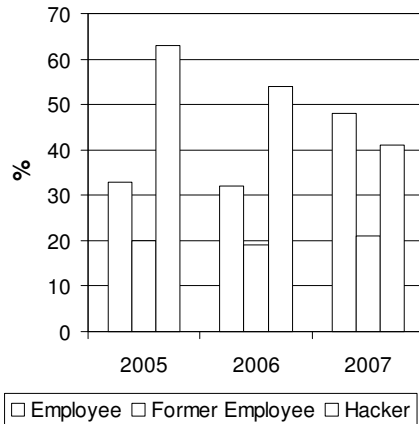
Slide 18

Trends - Globally Trend Around Identity Theft and the Risk of the Knowledgeable Insider

Insider threat is on the rise...

This year employees took over the number one spot as the most likely source of an information security event.

- In 2007, 48% of respondents pointed to employees vs. 41% to hackers.
- But in 2005 only 33% of respondents sighted employees as the most likely source vs. 63% for hackers.
- Key risk areas –admissions/ enrollment, collections, call centers, janitorial, computer programmers, benefits managers,



PricewaterhouseCoopers

Slide 19

Trends – Identity Theft & Social Engineering Global Risks

Identity theft and social engineering are risks in varying degrees.

	Total	North America	South America	Europe	Asia	Middle East & Africa
Identity Theft	9%	9%	11%	6%	10%	16%
Social Engineering	16%	16%	16%	14%	16%	17%

	South America		Asia					Middle East & Africa		
	Argentina	Chile	Australia	China	India	Malaysia	Singapore	Isreal	South Africa	UAE
Identity Theft	9%	17%	8%	11%	13%	14%	9%	7%	24%	33%
Social Engineering	12%	17%	15%	13%	26%	25%	11%	11%	35%	14%

PricewaterhouseCoopers

Slide 20

Section 4. Five Preventative Approaches to Limiting Exposure

PricewaterhouseCoopers

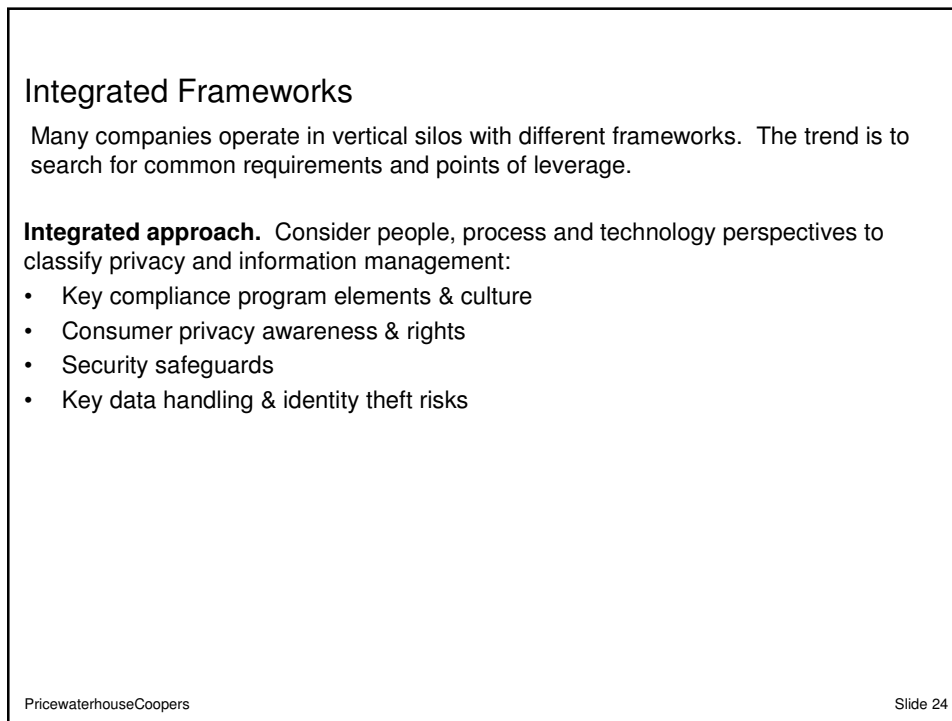
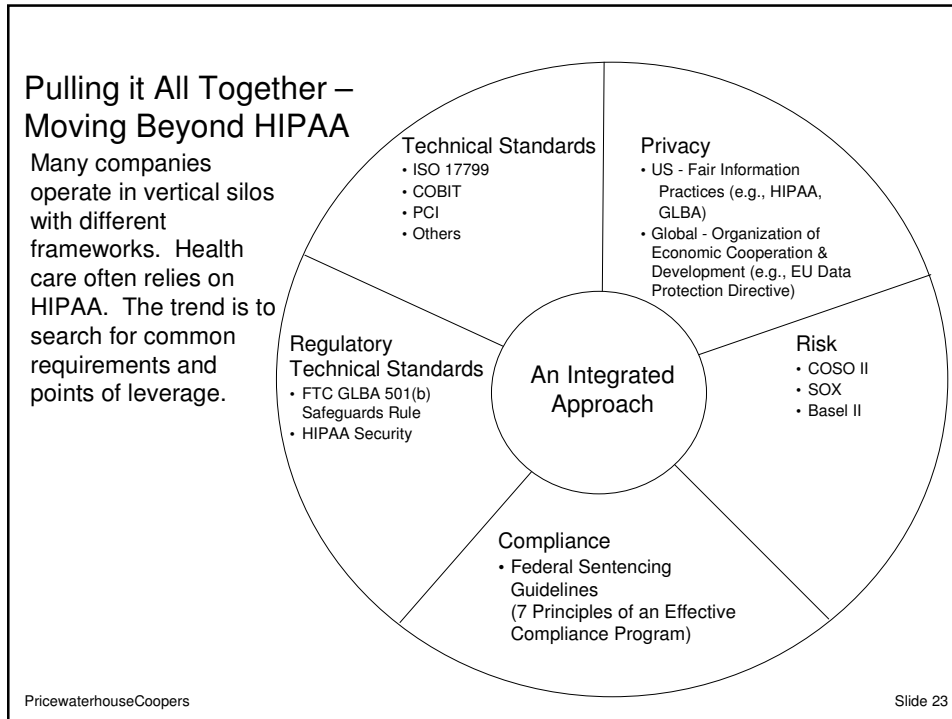
Trend #1 – Developing a Plan and Integrated Framework

- **A sound data protection and prevention plan is built on 5 key principles:**

- 1. Take stock. Know what personal information you have in your files and on your computers.**
- 2. Scale down. Keep only what you need for your business.**
- 3. Lock it. Protect the information that you keep.**
- 4. Pitch it. Properly dispose of what you no longer need.**
- 5. Plan ahead. Create a plan to respond to security incidents.**

PricewaterhouseCoopers

Slide 22



Trend #2 – Inventorying Location of High-Risk Data

Many companies are challenged to even know where their data is or even what is the nature of the data.

Data Inventories & Management	Consumer Products & Retail:	Consulting / Professional Services	Education / Non profit	Entertainment & Media:	Financial Services	Healthcare Insurance	Healthcare Provider	Pharma
Accurate inventory of user data kept	30%	32%	27%	28%	42%	38%	38%	42%
Accurate inventory of locations/ jurisdictions where data is stored	30%	30%	26%	26%	39%	38%	37%	37%
Keep inventory of all third parties using customer data	21%	24%	16%	16%	37%	45%	34%	31%
Require third parties to comply with your privacy policies	42%	38%	31%	28%	56%	64%	60%	54%

Data Mapping and Data Elements. Increasingly, companies are developing inventories of data owners (IT & Business), data elements, jurisdiction, data collection, use, retention and storage points.

PricewaterhouseCoopers

Slide 25

Breaking Information & Risk Down to Least Common Denominator

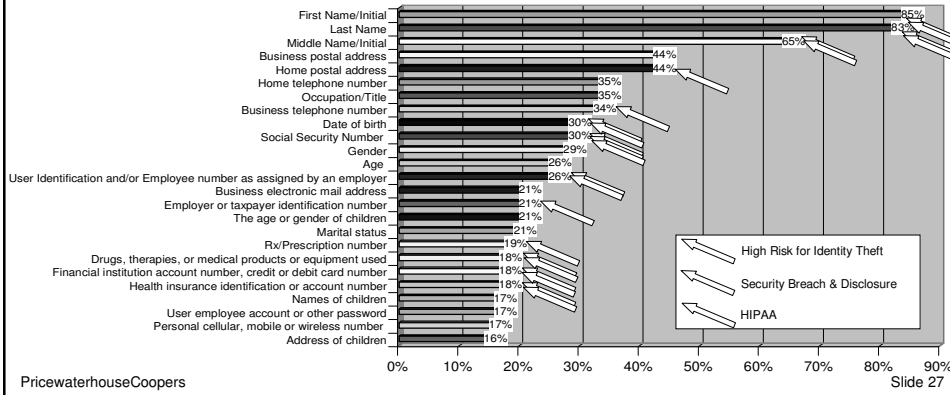
- **Bringing Order Out of Chaos . . . Aligning Investment with Risk.**
- **Data Elements.** Large and sophisticate companies are beginning to inventory certain data.
 - **HR/Benefits/Health Care.** HIPAA specifically enumerates 18 data elements that constitute Protected Health Information under the law.
 - **Identity Theft.** Certain data elements (e.g., Social Security, Driver's License, Credit Card Numbers and Health Insurance IDs) are at higher risk for identity theft.
 - **US State Security Breach & Disclosure.** 44 US states (and Japan) have laws requiring that notices be provided to individuals where an individual's name plus one of 14 other data elements (e.g., credit card, Social Security Number, health information, mother's maiden name, employee ID) may have been compromised.
 - **Credit Card Data.** Violations of Payment Card Industry information Security Standards and compromises of credit card data can result in fines and loss of processing privileges.
 - **Marketing Databases.** Proper access to and use of consumer marketing information (i.e., opt-out, refill reminders) have federal and state channel-specific and content-specific laws. Many of these laws also apply to business-to-business.
 - **International.** The EU Data Protection Directive and other global laws enumerate certain "Sensitive" data element (e.g., race or ethnic origin, health, religious beliefs and others).

PricewaterhouseCoopers

Slide 26

Example Excerpt Data Element (and Application) Inventory

- **Overview:**
 - **Application and Data Element Inventories and Critical.** To identify risks and compliance obligations, an inventory of applications, business processes and related high-risk privacy data elements are imperative.
- **Tactical/Practical Key to Success:**
 - **Focus on Global Set of Elements.** Avoid focus on just PCI, HIPAA, SSN and/or security breach laws. Focus on global set of more than 60 regulated elements or ones at high risk for ID theft.



PricewaterhouseCoopers

Slide 27

Trend #3 – Implementing Encryption

Often companies are planning to add or have added encryption

Encryption	Consumer Products & Retail	Consulting / Professional Services	Education / Non profit	Entertainment & Media	Financial Services	Healthcare Insurance	Healthcare Provider	Pharma
Transmission of data encrypted	60%	62%	47%	52%	75%	87%	67%	64%
Databases	51%	51%	45%	46%	51%	47%	39%	51%
File Shares	34%	40%	29%	29%	35%	30%	29%	31%
Laptops	38%	45%	25%	33%	54%	64%	37%	45%
Backup Tapes	41%	36%	31%	30%	44%	28%	33%	36%
Removable Media	27%	32%	22%	23%	32%	23%	22%	22%
Web transactions secured	46%	44%	39%	44%	61%	72%	41%	42%

- **Strategy.** Encryption is increasingly being implemented to avoid inclusion in US Security Breach & Disclosure Laws. Protections should consider beyond laptops – USB drives, discs, back-up tapes, retention, especially given requirements under MA 201 (for data in transit, wireless networks, laptops, mobile media and data at rest).
- **Unusual Results at Some Companies.** Often companies only focus on one type of data element in a one-off approach that is inefficient.
- **Use Justification & Destruction Not Considered Frequently.** There was some activity around FTC Destruction Rule for Credit Reports and now for eDiscovery.

PricewaterhouseCoopers

Slide 28

Trend #4 – Review All Technologies and Data Classification Schemes Based on New PHI Breach Law

Under new PHI breach notification law, "unsecured" PHI (which if compromised would lead to a breach notification) is defined to mean information not secured through a technology specified by HHS.

- **Secure?** HHS guidance by 4/18/09 specifying secure technologies. Until then, technology that renders information unusable, unreadable or indecipherable & based on ANSI standards are acceptable.
- **Data Classification.** To make consistent and operational, many are updating or building data classification schemes with required minimum controls for high-risk and regulated personal information (not just PHI).

Trend #5 –Identity Theft & Breach Response Protection

As more companies are experiencing breaches, they still remain relatively unprepared to respond and forensically investigate occurrence.

Breach Preparation	Consumer Products & Retail:	Consulting / Professional Services	Education / Non profit	Entertainment & Media:	Financial Services	Healthcare Insurance	Healthcare Provider	Pharma
Mechanisms in place to identify customers by state	18%	18%	12%	13%	36%	49%	20%	21%
Mechanisms in place to report security incidents to customers or	19%	28%	21%	19%	44%	55%	38%	39%

- **New Type of Incident Response Plans.** Often incident response plans are being redrafted to include security breaches and include specific high-risk data elements.
- **Common Tools.** Data loss prevention, detection and forensic monitoring devises are being commonly used for privacy, intellectual property protection and records/discovery analysis – email, data loss prevention, monitoring and others.

Questions?

• For the last 3 years, Forrester has recognized PwC as tied for or the sole leading privacy and security practice, noting our integrated approach to privacy, security and identity theft prevention as a leading factor

• In 2006 and 2007, ComputerWorld, recognized PwC as tied for the top consulting firm with a Privacy Practice
• Also, ComputerWorld recognized James Koenig as one of the top 25 privacy consultants in the World.

PricewaterhouseCoopers is ranked as the leading professional services firm providing information security and data privacy services to Global 2000 organizations. IDC, The Shifting Landscape: U.S. Information Security Services, 2003.

PricewaterhouseCoopers

Slide 31

Moving Beyond HIPAA: 10 Things Healthcare Organizations Need to Know About Breach Compliance & Medical Identity Theft*

© 2009 PricewaterhouseCoopers LLP. All rights reserved. "PricewaterhouseCoopers" refers to PricewaterhouseCoopers LLP (a Delaware limited liability partnership) or, as the context requires, other member firms of the PricewaterhouseCoopers network, each of which is a separate and independent legal entity. *connectedthinking is a trademark of PricewaterhouseCoopers LLP.

PRICewaterhouseCOOPERS 