HOW TO RESPOND TO A DATA BREACH: IT'S NOT JUST ABOUT HIPAA ANYMORE

The Fourteenth National HIPAA Summit™

March 29, 2007

Renee H. Martin, JD, RN, MSN

Tsoules, Sweeney, Martin & Orr, LLC

29 Dowlin Forge Road

Exton, PA 19341

610-423-4200

rmartin@tshealthlaw.com

TSMO

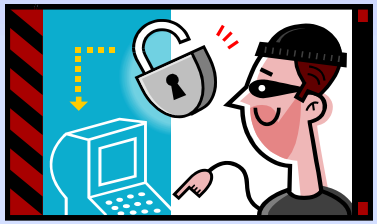
Data Breaches

- 2006 – Total Number of Reported Data Breach Incidents - 327
- Involved unprecedented disclosures of information security
- 100,453,730 total number of personal information potentially compromised

Data Breaches

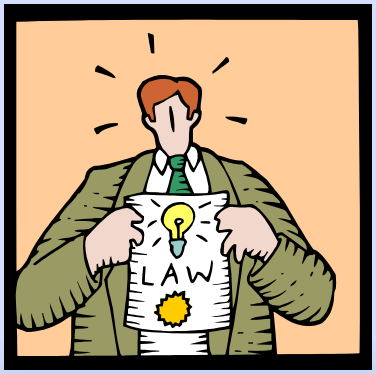
AARP Study – Analyzed 16 months of data breaches maintained by the Identity Theft Resource Center

- Breaches result of illegal or fraudulent attacks by hackers and careless practices
- Half of the breaches occurred at institutions of higher education – healthcare second
- Hackers most frequent cause of a breach
- Stolen computers the second most frequent cause of breaches



Data Breaches

- **Real Repercussions**
  - Loss of customer (patient) loyalty
  - Federal regulatory penalties/obligations
  - State regulatory penalties/obligations
  - Class action suits
  - Tort claims
  - Contractual damages/business loss



Federal Information Security Law

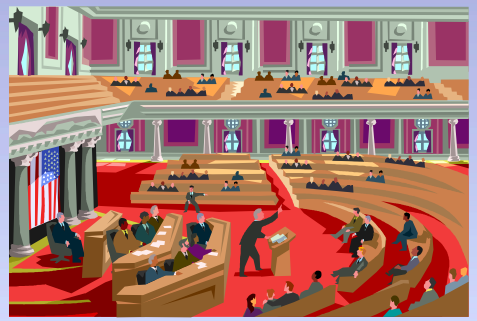
- HIPAA
- Computer Fraud & Abuse Law
- Electronic Communications Privacy Act

Federal Information Security Law

- USA Patriot Act
- Gramm – Leach Bliley
- FTC Act
- Sarbanes - Oxley

Federal Information Security Law

- **No Federal data breach legislation – several bills proposed**



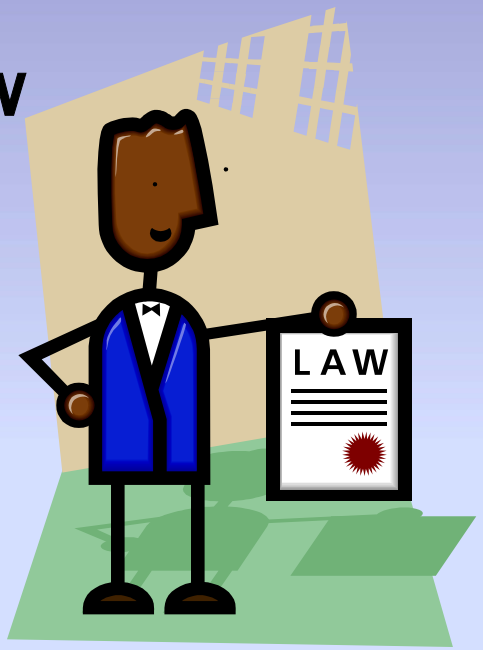
Federal Information Security Law

HIPAA and Data Breach Notification

- Covered entity:
  - has duty to "mitigate" impermissible uses and disclosures
  - has duty to account for impermissible uses and disclosures.
- Covered entity may use and disclose PHI with business associate; business associate must report to covered entity any breach of which it becomes aware
- No express requirement for business associate to notify others or to mitigate effect of breach

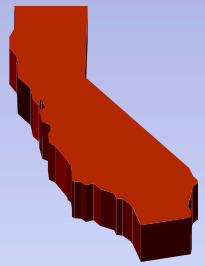
Federal Information Security Law

- HIPAA preemption and state law
  - State law more protective
  - State law not contrary



State Data Breach Notification

- 35 states have enacted - California led the way and is model/benchmark



- Seven states have pending legislation (AL, AZ, IL, MA, MI, MN, NJ, SC, WY)

California Data Breach Notification

- Targets entities not covered by GLBA, HIPAA or other similar Federal privacy laws

California Data Breach Notification

- Requires person, business or state agency that owns or licenses computerized data that includes personal information about California residents to implement and maintain reasonable security procedures and practices to protect personal information from unauthorized access, destruction, use, modification or disclosure

California Data Breach Notification

- **Application**
- **Any person, business or state agency that does business in CA and owns or licenses computerized data that contains personal information (PI).**
- **Implications for entities which possess but do not own PI**

California Data Breach Notification

- **Personal Information.** An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
  - SSN;
  - Driver's license number of CA ID card number; or
  - Account number, credit or debit card number, in combination with any required security code, access code, password (e.g., a PIN) that would permit access to an individual's financial account.

California Data Breach Notification

- **Security Breach Definition.** An unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of PI maintained by the person, business, or state agency.
- **Notification Obligation.** Disclose any breach of the security of the system following discovery or notification of breach in the security of the data to any resident of CA whose unencrypted PI was, or is reasonably believed to have been, acquired by an unauthorized person.

California Data Breach Notification

- **Third Party Data Notification.** If any entity maintains computerized data that includes PI that the entity does not own, the entity must notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the PI was, or is reasonably believed to have been, acquired by an unauthorized person.

- **Timing of Notification.** The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

California Data Breach Notification

- **Notice Provisions.** Notice of breaches may be provided by one of the following methods:

  - Written notice (form not specified).
  - Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 *et seq.* (E-Sign).

(Continued)

California Data Breach Notification

- Substitute notice, if the entity demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the entity does not have sufficient contact information. Substitute notice shall consist of all of the following:
  - E-mail notice when the entity has an e-mail address for the subject persons.
  - Conspicuous posting of the notice on the entity's Web site page, if the entity maintains one.
  - Notification to major statewide media.

(Continued)

California Data Breach Notification

- **Exception: Own Notification Policy.** Any entity that maintains its own notification procedures as part of an information security policy for the treatment of PI and is otherwise consistent with the timing requirements of the statute shall be deemed in compliance with the notification requirements of the statute if it notifies subject persons in accordance with its policies in the event of a security breach.

California Data Breach Notification

The California Office of Privacy Protection

Recommendations for Notice:

- A general description of what happened
- The type of personal information involved: SSN, driver's license or state ID card number, bank account number, credit card number, or other financial account number.
- What you have done to protect the individual's personal information from further unauthorized acquisition.

(Continued)

California Data Breach Notification

The California Office of Privacy Protection

Recommendations for Notice:

- What your organization will do to assist individuals, including providing your toll-free contact telephone number for more information and assistance.
- Information on what individuals can do to protect themselves from identity theft, including contact information for the three credit reporting agencies.
- Contact information for the California Office of Privacy Protection and/or the Federal Trade Commission for additional information on protection against identity theft.

California Data Breach Notification

Penalties

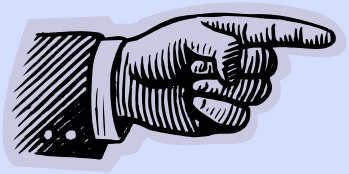
- Civil Action
- Civil Penalties
- Cumulative remedies

Data Breach

Most businesses have not addressed adequately how to respond.

What usually happens?

- "Circle Wagons"
- Finger Pointing
- Uncertainty



After the breach, too late!

Data Breach

What Should Happen?

- An Investigation
  - The scope and nature of the breach
  - The cause of the breach
- An Assessment of Potential Coverage of Specific State Statutes
- An Evaluation of Contractual Obligations
- Coordination of Possible Governmental and Media Concerns
- Liability Evaluation

The Investigative Phase

- What Happened?
  - How did it happen?
  - Who was involved?
- Precision and Specificity is Critical!!!
  - Notification and remediation rely on your ability to say with certainty what happened
  - Formal or informal statements from witnesses may be necessary
- How much time do you have to complete the investigation?

Assessment of Specific State Statutes

- Is statute electronic or broader in coverage?
- What data accessed?
- Was system accessed?
- Was data misappropriated or could it be misappropriated?
- Does it fit within "reasonable" expectation of harm as defined in state statute?
- Affirmative or negative tests on a state-by-state basis –critical issue

Assessment of Contractual Requirements

- What do your contracts say?
- Are you a business associate or covered entity?
- Are you a "third party"?
- Regardless of HIPAA, state law or contractual obligations, who should make notification?

Notice and Consumer Assistance

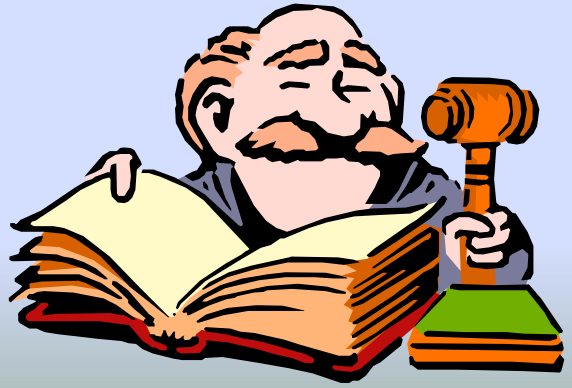
- What is the Scope of the Notice to be provided?
  - Must Notice be delayed while law enforcement officials investigate?
- What is statutory time frame for transmitting Notice?

- Will credit monitoring be offered?
  - Who pays?
- Will accounts be monitored?
  - Who pays?
- Do you have telephone line or contact person established?
- Are scripts and customer relations staff adequate?

Possible Government and Media Involvement

- There may be an affirmative duty to notify civil or criminal agencies or officials

- Notice to state consumer privacy agency or consumer protection agency and state attorney general's office



Possible Government and Media Involvement

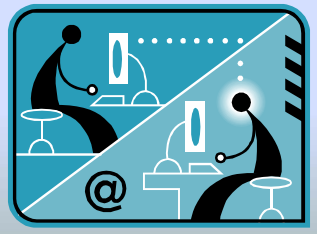
- The Media will go on a feeding frenzy

  - The buzz word is “Identity Theft”

- Leaking or misstatement of breach situation common
  - Significant reputation risk
  - Inclination by companies to downplay status

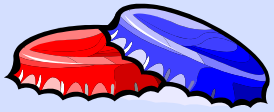
Liability Evaluation – Legal Risk

- Probability of Lawsuits
  - Good corporate citizen approach may not work – but necessary
- Specific statutory damages
- Administrative costs
  - Alternative notice procedures may be available under state law
- Is this an insurable loss?
- Utilize attorney/client privilege to conduct investigation
  - Manage your e-mails!!!!

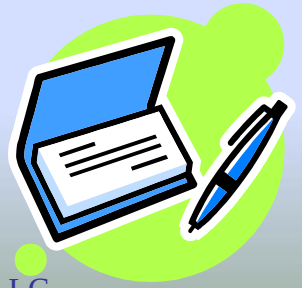


Contract Negotiations

- Implementation of security breach response plan
- Indemnification
- Damages and liability limitations – cap damages



- Termination
- Who pays for notification process?



Questions?

Questions??

Are There Any Questions?