

Davis Wright Tremain LLP 

**Responding to Your Worst
Security Breach Nightmare:
When Patient Information Is Stolen**

Thomas E. Jeffry, Jr., Esq.
Partner
Davis Wright Tremain LLP
Los Angeles, CA
213-633-4265
thomasjeffry@dwt.com

Rebecca L. Williams, R.N., J.D.
Partner
Davis Wright Tremain LLP
Seattle, WA
206-628-7769
beckywilliams@dwt.com



It Can Happen to Your Organization

- **“Patient data stolen from Kaiser”** *Vallejo Times Herald*, August 2006
- **“Computer Stolen From VA Subcontractor”** *Washington Post*, August 2006
- **“Patient records stolen”** *Press Register*, June 2006
- **“San Jose Arrest in theft of records
South Bay patients' medical data stolen”** *San Francisco Chronicle*, May 2005



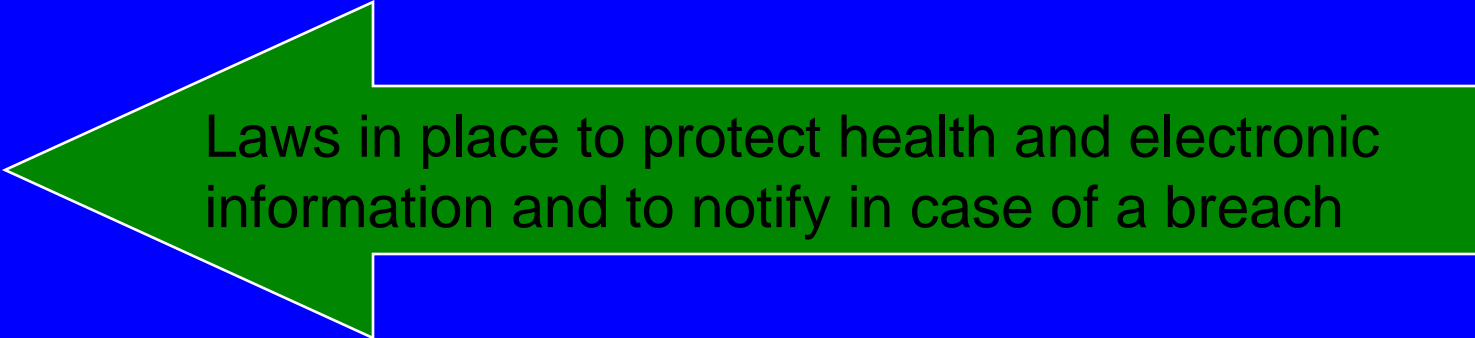
Finding the Balance



Strong push to electronic health information



Public and government outcry over privacy violations and identity theft



Laws in place to protect health and electronic information and to notify in case of a breach



Security Breaches Happen

- No such thing as perfect security
- Even with reasonable security measures, security breaches happen
 - Hackers
 - Lost or stolen technology, e.g., laptops, thumbdrives, PDAs
 - Disgruntled employees
- Need a prompt and effective response





Know the Laws that May Apply: HIPAA

- HIPAA - criminal and civil penalties for violations of the statute, Privacy Rule and/or Security Rule
- No private right of action but ...
- Privacy Rule prohibits uses and disclosures of PHI except as permitted or required by HIPAA
- Security Rule requires covered entities to
 - Protect against any reasonably anticipated
 - Threats or hazards to the security or integrity of ePHI
 - Impermissible uses and disclosure
 - Ensure confidentiality, availability and integrity of electronic PHI
 - Ensure compliance by a covered entity's workforce





Potentially Applicable Laws: HIPAA

- HIPAA Privacy Rule
 - Mitigation to the extent practicable
 - Sanctions
- HIPAA Security Rule
 - Mitigation of harmful effects of security incident
- No requirement to report





Potentially Applicable Laws: FTC Act and State Consumer Protection

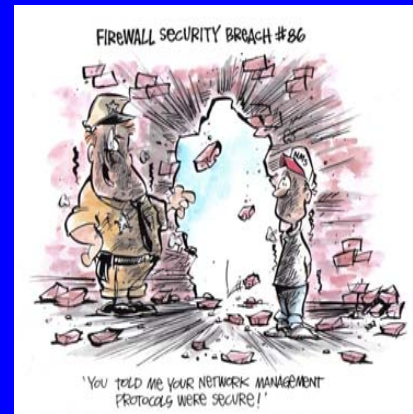
- Misrepresentation of privacy and security promises
- Failure to implement reasonable information security practices





Potentially Applicable Laws: Data Breach Notification

- California S.B. 1386 enacted in August 2002
- Increasing number of states enacting similar notification laws
- Specific triggers
 - Usually tied to security breach and electronic information
 - Sometimes requires notification only for breaches of unencrypted information
 - May be based on recipient
- Timing and content requirements





Potentially Applicable Laws: Confidentiality Laws

- Specific confidentiality requirements, particularly health care and financial information
- Superconfidentiality requirements in health care
 - Substance abuse (State and Federal)
 - Mental health and developmental disabilities
 - AIDS, HIV
 - Genetic information
- Federal Privacy Act
- Other laws
 - Be aware





Investigate the Breach

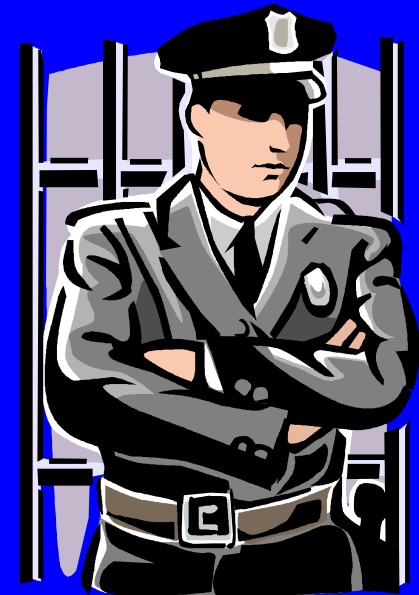
- Identify a single point person responsible for investigation
- Build a team
 - Identify needed expertise
- Inclusion of attorneys
 - In-house
 - Outside counsel
- Determine scope of breach
- Investigate fully
- Report internally





Notify Law Enforcement?

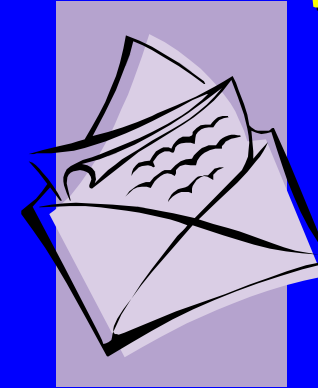
- Determine whether a crime seems likely to have been committed
- If so, law enforcement notification generally is prudent
- Be sure disclosures to law enforcement comply with applicable law, such as HIPAA
- Verify with law enforcement before notifying workforce, people affected or the public
 - Do not want to impede an ongoing investigation





Decision as to Whether to Notify

- Types of persons to be notified
 - Directors, members/shareholders
 - Workforce
 - Oversight agencies
 - Individuals whose information may have been affected
 - The public
- Each category requires a different analysis
- Considerations include:
 - Notification laws
 - Duties to mitigate (e.g., will notification diminish the chance of identity theft?)
 - Industry custom and practice
 - Ethical obligations
 - Preference of the organization





Timely Notification as Appropriate

- Carefully craft notice; consider including
 - Basic information about breach
 - Measures taken to address breach
 - Guidance on actions affected persons can take to protect themselves
 - Corrective action plan to avoid similar problem in the future
- Timing and content may be dictated by data breach or other laws
 - If law enforcement is involved, verify whether notification will interfere with investigation
- Be prepared to respond to those notified
 - Phone banks
 - Website
 - Adequate and trained staffing
- Point person for dealing with media or public (may not be the same as the person running the investigation)





Sanctions

- Did any workforce act or fail to act in a manner that should result in sanctions?
 - Up to any including termination
 - Sanctions to be consistently applied
- May prove helpful when dealing with oversight and enforcement agencies
- May want to consider a policy requiring workforce to cooperate fully in investigation (or face disciplinary action)





Fixing and Mitigating

- **Plan of correction**
 - **Need to assess causes of security breach**
 - What information was involved?
 - Who was affected?
 - How did it happen?
 - **Address immediate actions to remedy the breach at hand**

- **HIPAA Privacy and Security Rules require mitigation**
 - **Need to determine what actions, if any, will mitigate adverse effects**





Fixing and Mitigating

- Plan of Correction to avoid similar future breaches
 - Ask questions
 - Did all that information need to be on the laptop?
 - Security fixes
 - Revisit applicable policies, procedures, and protocols
 - Training/re-training of entire workforce
 - Concentrated training on more directly affected personnel
 - Other actions





Contacting Outside Agencies/ Cooperating in Outside Investigation

- Decision as to whether to notify outside agencies
 - May be required
 - May be recommendable
- Types of parties to be notified
 - JCAHO
 - State licensure
 - Attorneys General offices
- But not OCR (no process for self-reporting)





Continuing Operation

- Organization needs to continue operations while addressing security breach
- Often resources are strained





Davis Wright Tremaine LLP

Questions

