Regulation and Legal Requirements

William Mendez
March 24, 2004

Overview

- What are Legal Requirements?
- Big Picture
- Why are Legal Requirements Important?
- Examples of Legislation
- Consequences of Non-Compliance
- Costs of Compliance
- Conclusion
What are Legal Requirements?

Definition: Requirements mandated by legislation. Failure to comply with these requirements may lead to fines or other punitive actions.
Why are Legal Requirements Important?

- Impact on IT
  - Affects how you manage and protect your assets
  - Affects costs
  - Affects your risk analysis
  - Affects the management of internal controls

Legislation

- Sarbanes Oxley
- HIPAA
- California Breach Law (SB1386)
Sarbanes Oxley

- Enacted July 30, 2002
- Covers public corporations
- Motivation: Series of accounting scandals surrounding Enron, Tyco and other companies
- Goal: Restore public confidence in corporate governance

Sarbanes Oxley (cont)

Requirements

Section 302
- CEOs and CFOs must certify financial results

Section 404
- CEOs and CFOs must make assertions about the system of internal controls and mandatory documentation and evaluation
- Control objectives and techniques must be sufficiently documented
- Control objectives must be adequately designed to achieve the control objectives related to financial reporting

Section 802
- All audit or review work papers must be maintained for a period of 5 years from the end of the fiscal period in which the audit or review was conducted
- Relevant records include “work papers, documents that form the basis of an audit or review, memoranda, correspondence, communications, other documents, and records (including electronic records) which are created, sent, or received in connection with an audit or review and contain conclusions, opinions, analyses, or financial data relating to such an audit or review.”
What do these requirements mean?
- Must have properly designed and working internal controls
- Must have a way to monitor these controls
- Must have a data retention policy (along with the mechanisms to implement it)

What are internal controls?
- Policies and procedures designed to prevent or uncover errors and fraud

Classification
- Preventive
- Detective
- Corrective
Sarbanes Oxley

How do you assess internal controls?
- Need a criteria to compare with
- Sarbanes Oxley recommends using COSO: Committee of Sponsoring Organizations of the Treadway Commission
- COSO identifies 5 components of effective internal controls
  - Control Environment
  - Risk Assessment
  - Control Activities
  - Information and Communication
  - Monitoring

Sarbanes Oxley (cont)

Questions regarding data retention
- How is my data stored?
- Can I retrieve my data?
- How can I protect the integrity of the data?
Health Insurance Portability and Accountability Act (HIPAA)

Enacted in 1996
Title 1: addresses health insurance coverage, portability, and dealing with preexisting conditions
Title 2: Addresses issues of accountability, waste, and fraud

HIPAA

Relevant Goal for IT
- Establishment of Standards for the maintenance and transmission of patient health information (PHI)
- Title 2 (164)(c): PHI Data Privacy and Security
HIPAA

Main Sections

- Administrative Safe Guards
  - Propose a formal security management process (create, administer and oversee)
  - Ensure prevention, detection, containment and correction of security violations
- Physical Safe Guards
  - Workstation use
  - Workstation security
  - Disposal and reuse of electronic media
- Technical Safe Guards
  - Unique Employee IDs
  - Auditing access to PHI
## HIPAA

### 287 PHYSICAL SAFEGUARDS

<table>
<thead>
<tr>
<th>Standards</th>
<th>Sections</th>
<th>Implementation Specifications (R= Required, A=Addressable)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facility Access Controls</td>
<td>164.310(a)(1)</td>
<td>Contingency Operations (A)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Facility Security Plan (A)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Access Control and Validation Procedures (A)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maintenance Records (A)</td>
</tr>
<tr>
<td>Workstation Use</td>
<td>164.310(b)</td>
<td>(R)</td>
</tr>
<tr>
<td>Workstation Security</td>
<td>164.310(c)</td>
<td>(R)</td>
</tr>
<tr>
<td>Device and Media Controls</td>
<td>164.310(d)(1)</td>
<td>Disposal (R)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Media Re-use (R)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Accountability (A)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Backup and Storage (A)</td>
</tr>
</tbody>
</table>

## HIPAA

### TECHNICAL SAFEGUARDS (see § 164.312)

<table>
<thead>
<tr>
<th>Standards</th>
<th>Sections</th>
<th>Implementation Specifications (R= Required, A=Addressable)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>164.312(a)(1)</td>
<td>Unique User Identification (R)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Emergency Access Procedure (R)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Automatic Logoff (A)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Encryption and Decryption (A)</td>
</tr>
<tr>
<td>Audit Controls</td>
<td>164.312(b)</td>
<td>(R)</td>
</tr>
<tr>
<td>Integrity</td>
<td>164.312(c)(1)</td>
<td>Mechanism to Authenticate Electronic Protected Health Information (A)</td>
</tr>
<tr>
<td>Person or Entity Authentication</td>
<td>164.312(d)</td>
<td>(R)</td>
</tr>
<tr>
<td>Transmission Security</td>
<td>164.312(e)(1)</td>
<td>Integrity Controls (A)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Encryption (A)</td>
</tr>
</tbody>
</table>
California Security Breach Information Act (SB 1386)

- Enacted July 1, 2003
- A business must inform its customers when electronic data is compromised
- Covers companies that own or maintain personal information about California residents

SB1386

What information is protected?
- Person’s first name or initial and last name plus any one or more of the following:
  - Social Security Number
  - California Driver’s license or state ID
  - An account number credit or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account
When is notification required?

- SB 1386 requires notification “following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.”

How to notify?

- Letter
- Email (must comply with federal e-sign law)
- Public Notification
Consequences of Non-Compliance

- Sarbanes Oxley: $5 Million fine, 20 years imprisonment, or both
- HIPAA: Fines or imprisonment depending on which section was violated
  - Disclosing or obtaining individually identifiable health information could yield a $50K fine and up to a year in jail
- SB 1386: uncapped civil suit

Costs of Compliance

![Costs of Compliance Diagram](image)
Conclusion

- Legal Requirements Drive Design by
  - Affecting how you manage and protect your assets
  - Affecting costs
  - Affecting your risk analysis
  - Affecting the management of internal controls