4: REGULATORY DRIVERS

OBJECTIVES

1. Define and explain major regulatory requirements affecting policy.
2. Understand which and what type of regulations impact your organization.

DUE CARE

What it is:

- General principle addressing obligation of business managers to act reasonably and in the best interests of their organizations

What it means:

- Management can be held accountable for the efforts taken (or not taken) to comply with regulations, including those governing privacy safeguards and related policies.

HIPAA

What it is:

- Health Insurance Portability and Accountability Act of 1996
- A set of regulations governing health data privacy
- Affects medical service providers, insurance companies, companies, schools, etc.
- Intended to allow individuals to control access to and release of their personal medical information
- Specifies *what* must be protected, and *who* has to safeguard it, but not *how* data is protected

HIPAA

What it means:

- Healthcare industry participants must ensure that personal data is only disclosed subject to patient consent
- Applies to many health transactions that have been automated in recent years, as well as manual processes
- Extends responsibility to data in transit over and between networks
- Strongly implies needs for encryption, authentication, authorization, and other security provisions, but leaves implementation details to organizations.

HIPAA

What has to be done:

- Effective in April 2003, affected organizations must implement procedures to comply with the Privacy Rule
  - Includes consumer/patient notification, preferences, and explicit permission for release of protected health information (PHI)
- Since 2005, these same organizations must achieve compliance with the Security Rule
  - Establishes guidelines for the minimum requirements to ensure confidentiality, security and integrity of electronically stored and transmitted health information.
  - Covers electronic and non-electronic forms of information
  - Does not provide specific instruction on how organizations should safeguard PHI

GLBA

What it is:

- Graham-Leach-Bliley Financial Services Modernization Act of 1999
- A set of regulations governing financial data privacy
- Affects financial institutions and affiliated businesses working with personal financial data
- Particularly addresses sharing of non-public personal information by financial institutions
- Intended to allow individuals to control use and release of their personal financial information
- Specifies what must be protected, and who has to safeguard it, and acceptable compliance guidelines

GLBA

What it means:

- Financial institutions must disclose their privacy policies up-front and again at least annually
- Requires FI's to deliver privacy policy notices to consumers/customers to offer and describe opt-out provisions
- Holds FI's responsible for safeguarding customer data whether through normal business operations, theft, fraud, or exceptional circumstances

SARBANES-OXLEY

What it is:

- Public Company Accounting Reform and Investor Protection (Sarbanes-Oxley) Act of 2002
- A set of regulations governing financial reporting requirements for companies
- Reduces the time allotted for release of earnings and other financial report data

SARBANES-OXLEY

What it means:

- Senior management now requires more up-to-date understanding of all financial information
- Managers must certify and be accountable for the financial reports their companies issue
- Managers must describe and evaluate their internal controls for effectiveness
- All findings must be certified by external auditors
- Many former IT responsibilities elevated to business management

FISMA

What it is:

- Federal Information Security Management Act (Title III of E-Government Act of 2002)
- A set of organizational practices, roles, and responsibilities for government agencies related to information security.
- Applies to all federal agencies and contractors managing or maintaining federal systems.

FISMA

What it means:

- All federal agencies submit annual reports on security practices, controls, and level and extent of documentation.
- Agency-level scores given based on factors such as consistent and comprehensive implementation of practices, and effective use of controls.
- Responsibility for information security placed under federal CIOs, following standards and guidance produced by NIST.

CALIFORNIA SECURITY BREACH NOTIFICATION

What it is:

- SB 1386 passed in 2003 covering any person or business that conducts business in California
- Requires businesses to give public notice of information security breaches resulting in disclosure of personal information.
- Notification only must occur to California residents; however, 37 other states have now enacted similar laws
- Only exception is for encrypted data.
- Statute applies regardless of where the data is physically stored or where the breach occurs.

EUROPEAN UNION DIRECTIVES

- EU Data Protection Directive (1998)
- Imposes data privacy requirements on entities that transport data across national borders.
- Places data ownership and control in the hands of originating businesses.
  - Explicit permission for third-party data sharing
  - Disclosure/data sharing must be in the interest of the data subject
  - Applies to US companies that do business with the EU
  - Rules in US Dept. of Commerce “safe harbor” privacy framework

EUROPEAN UNION DIRECTIVES

- EU E-Commerce Directive (2000)
- Creates minimum requirements for selling to EU consumers and businesses online.
- Addresses both business practices and information transparency.
  - Mandatory business location and contact information
  - Reproduce-ability of online contract terms
  - Prompt notice of order confirmation
  - Local additional imposed by some EU member states

EUROPEAN UNION DIRECTIVES

- EU Electronic Communications Directive (2002)
- Creates a framework for an EU-wide effort to regulate unsolicited electronic mail or “spam.”
- Prohibits businesses without pre-existing customer relationships to solicit consumers unless they opt in.
- Makes illegal the common US business practice of sharing marketing leads between affiliated companies.
- Also constrains the use of “cookies” without explicit consumer notification.