

# Chapter 5

External Environment and  
Government Policy

# Learning Objectives

- Describe a justification for government intervention in business processes.
- List five major types of government intervention into healthcare business, and explain the need for government to invest in healthcare IM/IT.
- Describe the eight components of the administrative simplification portion of HIPAA.
- Assess your organization's readiness for transactions and code set development.
- Analyze why privacy and security are important and why IM/IT has a key role in protecting privacy and security.
- Assess four key questions to answer in developing privacy policies.
- Describe IM/IT leadership's role in responding to legislation.

# Concepts to Develop

- Justification for the government's role in healthcare IM/IT
- Select requirements of the Health Insurance Portability and Accountability Act (HIPAA)
- Healthcare IM/IT leadership roles
  - Leadership of IM/IT must develop a plan to anticipate and respond to the external environment's and government's direct, indirect, and substantial roles in healthcare operations.

# Justification for Government Intervention

- Government intervenes if markets fail to allocate resources effectively.
- Common reasons for intervention include
  - Public goods
  - Externalities
  - Imperfect Information
  - Monopoly

# Types of Government Market Intervention

---

## *Purpose*

---

Provide public goods  
Correct for externalities  
Impose regulations  
Enforce antitrust laws  
Sponsor redistribution programs  
Operate public enterprises

## *Government Initiative*

---

Funding of medical research  
Tax on alcohol and cigarettes  
Federal Drug Administration  
Limit hospital mergers  
Medicare and Medicaid  
Veterans Administration hospitals

---

*Source:* Reprinted from Feldstein (2001). Used with permission from Health Administration Press, Chicago.

# Benefits of Government Involvement

- No compelling business case exists for investment in health information technology. The savings from implementing health information technology do not go to providers but rather to benefit insurers and others.
- For system benefits from IM/IT investment to be seen, all components of the fragmented U.S. healthcare delivery system must participate. Without this participation, benefits are incomplete. Interoperability among providers is a necessary step for true sharing to occur, and government needs to impose common communication standards.
- Fraud and abuse regulations do not allow physicians to receive subsidies from hospitals.

# HIPAA Portability and Simplification Sections

- Establishes national standards for electronic healthcare transactions and national identifiers for providers, health plans, and employers
- Addresses the security and privacy of health data
- Aims to improve the efficiency and effectiveness of healthcare system via electronic data interchange

# Elements of Simplification (CMS 2005b)

- Standards for electronic health information transactions
- Mandate on providers and health plans, and timetable
- Privacy
- Pre-emption of state law
- Penalties

# Standards (CMS 2005b)

- Within 18 months of enactment, the Secretary of HHS is required to adopt standards from among those already approved by private standards-developing organizations for certain electronic health transactions, including claims, enrollment, eligibility, payment, and coordination of benefits.
- These standards also must address the security of electronic health information systems.

# Provider and Health Plan Mandate (CMS 2005b)

- Providers and health plans are required to use the standards for the specified electronic transactions 24 months after they are adopted.
- Plans and providers may comply directly, or may use a healthcare clearinghouse.
- Certain health plans, in particular workers compensation, are not covered.

# Privacy (CMS 2005b)

- The Secretary is required to recommend privacy standards for health information to Congress 12 months after enactment.
- If Congress does not enact privacy legislation within 3 years of enactment, the Secretary shall promulgate privacy regulations for individually identifiable electronic health information.

# Pre-Emption of State Law (CMS 2005)

- The bill supersedes state laws, except where the Secretary determines that the State law is necessary to prevent fraud and abuse, to ensure appropriate state regulation of insurance or health plans, addresses controlled substances, or for other purposes.
- If the Secretary promulgates privacy regulations, those regulations do not preempt state laws that impose more stringent requirements.
- These provisions do not limit a State's ability to require health plan reporting or audits.

# Penalties (CMS 2005b)

- The bill imposes civil money penalties and prison for certain violations.

# Privacy

- Privacy Act of 1974 established key provisions
- Current concept of privacy
  - Control of information concerning personal life
  - Freedom from intrusion upon "seclusion"
  - Limits on publicity that places one in a false light
  - Prevention of identity theft and likeness
  - Right to keep personal information confidential

# Evolving Leadership Roles

- Environmental scanning and organizational education
- Information security policies and procedures
- Disaster protection and recovery procedures
- Protection of information privacy and confidentiality

# Environmental Scanning and Organizational Education

- Determine breadth and scope of impending or actual legislation.
- Assess current organizational readiness for impact.
- Perform gap analysis within organization.
- Recommend strategies to meet legal/regulatory changes.
- Identify clinical and other resources within the organization that will be necessary in meeting standards.
- Outline timeline for implementation with key dates and milestones.

# Information Security Policies and Procedures

- Healthcare organizations must establish enterprisewide standards to maintain data security and protect the privacy and confidentiality of health information (patient records).
  - Protect against system failures or external catastrophic events, such as fires, storms, deliberate sabotage, and other acts of God, where critical information could be lost
  - Control access to computer files by unauthorized personnel

# Disaster Protection and Recovery Procedures

- Steering committee must ensure that effective data backup and recovery procedures are implemented.
- CIO develops a data backup plan for approval by the steering committee.
  - The plan should specify which files require duplication, frequency of duplication, and recovery procedures to be used if catastrophic events occur.
- Disasters include
  - Natural
  - Terror attacks
  - Computer viruses

# Protecting Information Privacy and Confidentiality

- **Physical Security**
  - Hardware
  - Data files
- **Technical safeguards**
  - Passwords
  - Encryption
  - Audit logs
- **Management policies**
  - Written security policy
  - Employee training
  - Disciplinary actions for violations