CHAPTER

3

GOVERNMENT POLICY AND HEALTHCARE REFORM

Learning Objectives

1. Describe a justification for government intervention in business processes.
2. List five major types of government intervention into the healthcare business, and explain the need for government to invest in healthcare information management and healthcare information technology (HIT).
3. Describe the eight components of the administrative simplification portion of the Health Insurance Portability and Accountability Act.
4. Assess your organization's readiness for transactions and code set development.
5. Analyze why privacy and security are important and why HIT has a key role in protecting privacy and security.
6. Assess four key questions to answer in developing privacy policies.
7. Describe HIT leadership's role in responding to legislation.

Overview

Much has been written regarding the details of the federal, state, and local government policies that have direct and indirect influences on healthcare information technology (HIT) and its leadership in healthcare organizations (Blumenthal 2006; Feldstein 2001; Goldsmith, Blumenthal, and Rishel 2003; Kleinke 2005; Poon et al. 2006; Taylor et al. 2005). This chapter does not present an exhaustive list of those impacts. Its goal is to provide HIT leadership with the awareness of the potential effects of healthcare legislation on HIT business practices; the tools to identify and respond to current healthcare legislation; and the strategic vision to plan for future challenges that may arise from government interventions. The chapter has three sections:

1. *Government's role in HIT.* This section provides the justification for government intervention in business processes. Understanding why government gets involved will assist you in responding to legislation and anticipating future actions.
2. *Specific healthcare legislations.*
   a. Health Insurance Portability and Accountability Act (HIPAA) of 1996. This major set of legislative and administrative interventions has fundamentally changed HIT for the last decade and will likely change it in the future. It is a complex array of interventions that have been implemented in ways not fully anticipated when the legislation was passed in 1996. This section presents some basic policies and procedures designed to respond to select HIPAA requirements.
   b. American Recovery and Reinvestment Act's Health Information Technology for Economic and Clinical Health Act. This legislation arose from the economic crisis of 2007–2009 but became an enabler, nonetheless, of electronic health record adoption in the United States.
   c. Patient Protection and Affordable Care Act of 2010. This controversial health reform legislation is designed to expand coverage to the uninsured and to improve quality of care and provider accountability.
3. *HIT leadership roles.* The external environment and government have direct, indirect, and substantial roles in healthcare operations. Leaders must understand those roles today and anticipate roles in the future. This section presents an action plan for HIT leadership.

Government's Role in HIT

Three questions must be asked in assessing the role of government in HIT:

1. Why does the government (at any level) get involved in healthcare or any business practice? Is there justification for government intervention?
2. If yes, how much and what types of intervention are justified?
3. What triggers those interventions?

The easy answer to these questions is that the government recognizes the challenges that the healthcare field faces regarding cost, quality, and access to care (see Chapter 2 or Gauthier and Serber [2005]). Further, the government has an obligation to intervene to provide access to high-quality, affordable care to all residents.

Justification for Government Intervention

The generic argument for government intervention is that the marketplace does not perform its normal function of optimizing resource-production efficiency and resource-allocation decision making as classical economics theory suggests (Santerre and Neun 2004). As a result of the market's failure, government can—and some say should—intervene to fix the problem. Key reasons for intervention include problems with public goods, externalities, imperfect consumer information, and monopoly. Public goods are those that producers cannot easily exclude people from consuming, and consumption by one person does not reduce the availability for others to consume. A classic example is national defense, but medical research that leads to cures for disease is another. Externalities are costs or benefits related to a market action that parties not related to the transaction incur. For example, cigarette smoking may impose costs on those not involved in the decision to smoke. Imperfect information may give rise to government involvement in markets because people are concerned that profit-seeking businesses may take advantage of people's inability to make informed choices. In each of these cases, the market does not reliably provide the optimal quantity. (See Santerre and Neun [2004] for an extensive discussion of these issues.)

If the market fails to produce a good or service for any of these reasons, government is empowered to intervene in the public interest. Generally, the "fix" is to develop and implement policies that approximate what the market solution would generate, if possible. For healthcare, that intervention is justified because of asymmetric information between purchasers and providers and significant uncertainty about future need for services (Arrow 1963; Poterba 1996). However, some have argued that government interventions are designed to benefit those special interests that influence politicians rather that society as a whole (Blumenthal 2006; Feldstein 2001; Goldsmith, Blumenthal, and Rishel 2003; Kleinke 2005; Taylor et al. 2005).

Examples of the range of government intervention are included in Exhibit 3.1. Correcting externalities has been one of the major reasons for government intervention. HIPAA, described later in this chapter, can be considered an intervention to force a market solution that would not occur without direct government support. Funding for medical research is a more traditional example of this type of intervention and is briefly described as it relates to funding for HIT. The other categories in the exhibit are not directly relevant to this book but are still worthy of note.

A significant amount of research in HIT has been funded by the federal government. A primary source of this funding for research and demonstration projects comes from the National Library of Medicine (NLM, www.nlm.nih.gov). The importance of the NLM to current initiatives and emerging features of HIT make it a major change agent. HIT leadership should be

EXHIBIT 3.1 Types of Government Market Intervention

Purpose	Government Initiative
Provide public goods	Funding of medical research
Correct for externalities	Tax on alcohol and cigarettes
Impose regulations	Federal Drug Administration
Enforce antitrust laws	Limit hospital mergers
Sponsor redistribution programs	Medicare and Medicaid
Operate public enterprises	Veterans Administration hospitals

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

familiar with NLM funding priorities. Exhibit 3.2 presents the eight primary functions of the NLM. Assisting healthcare organizations with developing the data systems to support both their clinical operations and health services research is a major portion of NLM's charge. Using the justification for government intervention argument, the government funds these (and other) crucial activities because it believes that private organizations will not spend sufficiently on them. Further, the findings from these efforts will benefit the entire US healthcare system by enabling the development and testing of new technologies and infrastructure support.

EXHIBIT 3.2 Primary Functions of the National Library of Medicine

The National Library of Medicine

1. assists the advancement of medical and related sciences through the collection, dissemination, and exchange of information important to the progress of medicine and health;
2. serves as a national information resource for medical education, research, and service activities of Federal and private agencies, organizations, and institutions;
3. serves as a national information resource for the public, patients, and families by providing electronic access to reliable health information issued by the National Institutes of Health and other trusted sources;
4. publishes in print and electronically guides to health sciences information in the form of catalogs, bibliographies, indexes, and online databases;
5. provides support for medical library development and for training of biomedical librarians and other health information specialists;
6. conducts and supports research in methods for recording, storing, retrieving, preserving, and communicating health information;
7. creates information resources and access tools for molecular biology, biotechnology, toxicology, environmental health, and health services research; and
8. provides technical consultation services and research assistance.

SOURCE: Reprinted from the National Library of Medicine (2004).

Government Intervention in the Healthcare Field

For most industries, the government largely allows the market to determine costs, efficiency, quality, availability, and firm survival. With the exception of enforcing property rights and legal contracts, the government's role is minor.

Healthcare is different from other industries, however. The government gets involved in healthcare—and, by extension, HIT—because the government has a broad obligation to protect the health and welfare of the population. That obligation extends beyond ensuring that markets function and property rights are enforced (Feldstein 2001). Finding that the health of the population is at risk makes intervention to improve patient safety vital. Evidence that this risk is real comes from a series of prestigious studies, such as the Institute of Medicine's 1999 and 2001 reports. Further, published estimates that nearly 50 million people are uninsured and many more are underinsured (DeNavas-Walt, Proctor, and Smith 2012; Gauthier and Serber 2005) bring another call for government intervention. Lack of insurance has an effect on the health of the population because lack of insurance may actually lead to preventable morbidity and mortality (a negative health outcome), which in turn cost the US healthcare system more than $65 billion per year (Ayanian et al. 2000; IOM 2003).

As discussed in earlier chapters, healthcare costs have been rising rapidly both in absolute terms and relative to the gross domestic product. These increases in cost are largely paid by governments; thus, budget considerations drive government interest as well. In 2010, 39.2 percent of personal health expenditures were paid by Medicare and Medicaid alone. All levels of government have a major stake in payment rates (CMS 2012b). The conclusion is that quality, access, and cost provide a justification of the government's role in healthcare and thus in HIT. (See Chapter 2 for more details on the expenditures for healthcare services.)

Government and Business Practice

Given that government intervention can be justified, how much and what types of intervention are justified? With respect to HIT, patient information privacy and security are the major foci of government intervention. The argument is that social interest in having patient healthcare information protected cannot be left to individual providers. Good business practice dictates that much of what comes under the guise of government intervention should be followed irrespective of the regulations. As addressed in detail in the next section, HIPAA has, among other features, enhanced privacy regulation.

Because healthcare delivery organizations are responsible for the health and welfare of their patients, it only makes sense to adopt strict privacy standards even in the absence of government regulation. Therefore, information system managers in healthcare facilities must develop policies and procedures to protect the security of information contained in automated systems throughout the organization.

Government can extend into healthcare business practices in a number of potential ways. Goldsmith, Blumenthal, and Rishel (2003) argue for the need for government-sanctioned and government-supported standardization of at least communication protocols and nomenclature. Without a direct government role, healthcare organizations will adopt technology slowly and in a haphazard fashion. Blumenthal (2006) provides three business arguments justifying government intervention. First, no compelling business case exists for investment in HIT. Better performance is not routinely rewarded in healthcare, and, in fact, poor performance and providing more services generate greater revenue. The savings from implementing HIT do not go to providers but rather benefit insurers and others. Second, for real system benefits to be seen, all components of the fragmented US 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. Third, fraud-and-abuse regulations do not allow physicians to receive subsidies from hospitals. Blumenthal (2006) makes a strong case for the failure of the market to achieve the desired results, and thus government must become more actively involved. HIT leadership must be aware of specific government interventions to effectively manage their organization.

The bottom line is that government has intervened in healthcare markets in significant ways, such as through the Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH) Act, and the Patient Protection and Affordable Care Act (ACA). The issue with regard to HIT intervention, however, is still somewhat open, but a growing body of evidence suggests that HIT investment will have positive results (Buntin et al. 2011). Economic recovery funding through the HITECH Act implicitly assumes that this investment is good for quality and potentially for cost savings.

Specific Healthcare Legislations

Health Insurance Portability and Accountability Act

As an example of legislation that has had far-reaching effects on HIT, HIPAA has no equal. Begun as a mechanism to ensure that individuals could retain

access to health insurance when they changed jobs (portability) (Flores and Dodier 2005; Schmeida 2005), HIPAA also contains a second provision called *administrative simplification* that has far greater impact (CMS 2005a):

> The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) required the Department of Health and Human Services (HHS) to establish national standards for electronic healthcare transactions and national identifiers for providers, health plans, and employers. It also addressed the security and privacy of health data. As the industry adopts these standards for the efficiency and effectiveness of the nation's healthcare system will improve the use of electronic data interchange.

As this general provision indicates, HIPAA anticipated the development of electronic record keeping in healthcare. The healthcare field was not able internally to develop the standards and rules governing these new technologies for collecting, storing, and transmitting health information (another example of potential market failure mentioned earlier). Many realized that strict government controls would have to be put in place to enable healthcare providers to develop systems that met internal needs and facilitated the transfer of information across institutions (Blumenthal 2006; Goldsmith, Blumenthal, and Rishel 2003; Kleinke 2005). The electronic medium also raised concerns with security and privacy that the government felt it should address. In simple terms, administrative simplification involved setting standards, mandating health plan and provider compliance, and establishing privacy elements (CMS 2005b).

The complete text of HIPAA's Summary of Administrative Simplification Provisions is provided in Exhibit 3.3. Each of the five provisions presented in the exhibit is important because of what it implies. While the translation of these broad provisions to policy details has evolved incrementally since the passage of HIPAA in 1996, the details are now emerging as a result of a series of negotiations among all of the interested parties. Exhibit 3.4 shows the eight components of the administrative simplification provisions that were promulgated to meet the five provisions listed in Exhibit 3.3.

The HIPAA overview reveals specific details of these standards and the timing of their implementation (CMS 2005a). Steps to achieving the goals of improving patient quality and enhancing efficiency through the use of electronic records were developed in stages. The first step was to make employers obtain a national identification number for healthcare transactions. Next, providers were required to have a commonly determined standard identifier—the National Provider Identifier (NPI). These rules set the stage for creating a regional or national data set of electronic information transmission by uniquely identifying the payer source and the provider. This seems

EXHIBIT 3.3
HIPAA's Summary of Administrative Simplification Provisions

Standards for electronic health information transactions. 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.

Mandate on providers and health plans, and timetable. 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 health care clearinghouse. Certain health plans, in particular workers compensation, are not covered.

Privacy. 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. 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 pre-empt state laws that impose more stringent requirements. These provisions do not limit a State's ability to require health plan reporting or audits.

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

NOTE: Provisions in the original legislation have been modified by subsequent legislation, including the ACA.
SOURCE: Reprinted from CMS (2005b).

EXHIBIT 3.4
Eight Major Components of HIPAA Administrative Simplification Provisions

1. Employer-identifier standard
2. Enforcement
3. National provider-identifier standard
4. Security standard
5. Transaction and code sets standard
6. Place-of-service codes for HIPAA transactions
7. Health insurance reform for consumers (HIPAA Title I)
8. Medicaid HIPAA administrative simplification

SOURCE: Information from CMS (2005a).

insignificant when viewed from within a healthcare organization because they have always used unique numbers to identify patients and to keep patient records distinct. The NPI was novel when applied across organizations, however. The timing of the NPI mandate is current in relation to this discussion in that after May 23, 2007, "healthcare providers may only use their NPIs to identify themselves in standard transactions" (CMS 2005c).

Transactions and *code set standards* warrant additional commentary because they are so vital to the effective implementation and use of the electronic record. The precise definition of these standards is also still in flux. According to the Centers for Medicare & Medicaid Services (CMS 2005d),

> Transactions are activities involving the transfer of healthcare information for specific purposes. Under the Health Insurance Portability & Accountability Act of 1996 (HIPAA), if a healthcare provider engages in one of the identified transactions, they must comply with the standard for that transaction. HIPAA requires every provider who does business electronically to use the same healthcare transactions, code sets, and identifiers. HIPAA has identified ten standard transactions for Electronic Data Interchange (EDI) for the transmission of healthcare data. Claims and encounter information, payment and remittance advice, and claims status and inquiry are several of the standard transactions. Code sets are the codes used to identify specific diagnosis and clinical procedures on claims and encounter forms. The HCPCS, CPT-4 and ICD-9 codes with which providers are familiar, are examples of code sets for procedures and diagnose.

This generic statement gives rise to an array of specific rules designed to enable organizations to collect data in a consistent manner. Unless everyone uses a common nomenclature for defining all clinical and administrative terms, there will be no capacity to communicate. *Interoperability* is the term that describes the goal to its fullest extent. To assist providers and others in this pursuit, CMS has provided information on the web that can be easily accessed and applied. The posted information is a series of checklists to be used by healthcare organizations to determine their readiness; download the information from www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/EducationMaterials/Educational-Materials.html. In addition, CMS makes available a series of ten documents, listed in Exhibit 3.5, to assist organizations in dealing with issues appropriate to their particular need. (Discussing these documents is beyond the scope of this book; however, HIT leadership must be aware of their existence and importance.)

The Need for Information Privacy and Security

HIT "systems contain sensitive information. Clinical systems process medical information about individual patients; human resources information systems

EXHIBIT 3.5
Checklist Aids for Transactions and Code Set Development

The HIPAA Information Series for Providers consists of ten papers that can aid healthcare organizations in transactions and code-sets development as well as other HIPAA issues:

- HIPAA 101
- Are You a Covered Entity?
- Key HIPAA Dates and Tips
- What Electronic Transactions and Code Sets Are Standardized Under HIPAA?
- Is Your Software Vendor or Billing Service Ready for HIPAA?
- What to Expect from Your Health Plans
- What You Need to Know About Testing
- Trading Partner
- Final Steps for Compliance with Electronic Transactions and Code Sets
- Enforcement

These documents can be downloaded from www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/EducationMaterials/EducationalMaterials.html.

contain personal information about employees; and financial and decision-support systems include proprietary data used for planning, marketing, and management of the enterprise" (Stahl 2003). HIPAA has placed special emphasis on privacy, and the implications of safeguarding privacy to HIT leadership are expansive.

To give some idea of the nature and extent of privacy and security issues even after HIPAA's enactment, the Health Privacy Project (www.healthprivacy.org) has compiled anecdotes reported in the national press. The sheer number of events suggests their importance. In 2012 *Healthcare Finance News* reported the top ten security breaches for that year (McNickle 2012). These breaches affected many institutions, including the Utah Department of Health, Emory Healthcare, and the University of Arkansas for Medical Sciences. Following are examples from the Health Privacy Project's (2007) web publication, *Health Privacy Stories:*

- "The California state Department of Health Services inadvertently revealed the names and addresses of up to 53 people enrolled in an AIDS drug assistance program to other enrollees by putting benefit notification letters in the wrong envelopes. . . . The department learned about the mix-up after 12 people in the drug assistance program phoned to say they had received letters addressed to someone else. . . . The department is looking into ways to make the system more foolproof, such as using envelopes with window addresses, said health services Director Sandra Shewry. HIV/AIDS services and advocacy groups said this was the first known breach of that database. 'I would hope this is an anomaly,' said Jeff Bailey, director of client services for AIDS Project Los Angeles" (Engel 2007).
- "A desktop computer containing personal information for up to 38,000 patients treated at Veterans Affairs Department medical centers in Pittsburgh and Philadelphia over the past four years was reported missing from the Reston, VA offices of VA contractor Unisys Corp. The VA and Unisys [say] the computer contained names, addresses, Social Security numbers and dates of birth. It may also have included insurance carrier and billing information, claims data and medical information" (Robeznieks 2006a).

Needless to say, ensuring the security of clinical information systems must be a top priority for healthcare leaders and HIT managers alike. Clinical information systems refer to the following types of health and healthcare records:

1. *Patient care systems* include information technology used in the course of providing care, services, or treatments, such as order entry and results reporting; electronic medical records; and lab, pharmacy, and radiology systems. Data contained in these systems—including medical histories, medication lists, physician orders, diagnoses, treatment plans, and test results—are extremely private and thus should be accessible only to those involved in care delivery. Breach of security in this instance has legal and ethical ramifications for the healthcare delivery organization.
2. *Public health information systems,* according to Stahl (2003), "support disease prevention and surveillance programs. Protecting public health requires the acquisition and storage of health-related information about individuals. Public health benefits sometimes conflict with threats to individual privacy. Individuals concerned about privacy who avoid clinical tests and treatments may endanger the health of others in the community." For example, a person with a sexually transmitted infection may opt to not test and/or report the presence of the infection, which could then lead to the spread of the disease (Gostin, Hodge, and Valdiserri 2001). A security breach of public health information systems could lead to a person or groups facing discrimination in employment or insurance eligibility.
3. *Medical research information systems* are repositories of medical diagnoses, health conditions, disease data, risk factors, and other health-related details culled from patient records. The purpose of such a

system is to enable clinical researchers and other investigators to understand disease risks, patterns, and contributing factors observed in a patient population. Lau and Catchpole (2001) emphasized the importance of respecting the patients' privacy rights as well as protecting the information contained in these systems by restricting access and use to authorized personnel.

Following are some of the ways healthcare delivery organizations have addressed privacy concerns to comply with HIPAA standards:

- Form HIPAA task forces.
- Install a new compliance office or function dedicated to managing HIPAA-related challenges, or designate an existing office or function (e.g., chief information officer, medical records, risk management) to address or prevent issues (Marietti 2002).
- Use information system software designed by a vendor to meet the specific purpose, needs, and concerns identified by the organization. In this way, HIPAA patches to existing programs, and some in-house work is required to ensure the applications interface with one another (Wilson and McPherson 2002).
- Implement changes to some business processes and procedures. Marietti (2002, 55) projected that "80 percent to 85 percent of HIPAA compliance issues will depend on adjusting human behavior."

Findings from studies of the HIPAA regulations have emerged. First, the immediate impact has been on the research community. Evidence suggests that HIPAA compliance makes recruitment and retention of subjects into research projects more difficult (Wipke-Tevis and Pickett 2008). Second, some specific examples now exist regarding how process improvements (automated access verification) can assist organizations to demonstrate compliance (Hill 2006). Third, the change process is still incomplete because privacy and security rules are being revised/updated frequently, such as a new rule announced in January 2013 (HHS 2013). Checklists are still being published to help organizations meet HIPAA requirements (HIPAA Survival Guide 2013).

A number of studies have examined the impact of privacy rules on healthcare organizations, giving rise to a set of inappropriate responses (as observed by consultants) related to privacy (Upham and Dorsey 2007). Some concerns center on the application of privacy rules to other activities or innovations in healthcare. For example, in 2007 Paul Tang, then the chair of the board of the American Medical Informatics Association, indicated that electronic health record vendors often included contract provisions that may

require providers to violate patient privacy standards (Conn 2007). Similarly, in the wake of mass tragedies, access to the perpetrator's health record often is cited as a reason to relax privacy constraints. Peel (2007) discussed this issue in the context of the Virginia Tech massacre in April 2007, in which a student killed 32 people on that campus. Peel concluded that privacy constraints would not likely prevent these events. More recently, there is the case of James Holmes—the gunman who opened fire at an Aurora, Colorado, movie theater, killing 12 and injuring about 50 people. Prior to the shooting, Holmes was reportedly being seen by a mental health specialist at the University of Colorado, where Holmes was a student (Meyer and Ingold 2012). The specialist contacted a university threat-assessment team but did not invoke a "72-hour psychiatric hold" because Holmes was leaving the university. Under pressure from news sources that are trying to piece together the events that led up to the tragedy, the University of Colorado released thousands of e-mails related to Holmes. However, the university did not make available any records or documents related to the crime or Holmes's mental health status (Meyer and Ingold 2012). As consumers continue to provide information over the Internet, the collection, availability, and security of their data will remain a major concern (Nelson 2006).

At the level of information sharing across organizations was a study commissioned by the California Healthcare Foundation to look at privacy from the perspective of developing regional health information organizations (RHIOs). The study was trying to determine what needed to be done at the systems level to facilitate RHIO development. It resulted in a number of findings and substantial recommendations on developing and implementing security policies for RHIOs. The analyses identified the following four key questions that must be addressed to develop privacy policies (Rosenfeld, Koss, and Siler 2007):

1. Who will have access to patient information?
2. Which information will be accessible?
3. What are acceptable purposes of patient information exchange?
4. What circumstances justify patient information exchange?

In addition, the study reported a number of common elements that are important to consider in developing privacy policies across organizational entities, including the following:

- Privacy policies are local.
- Organizations participating in the RHIO influence the privacy policies.
- Privacy policies need to be developed early and revisited often.
- Work on privacy policies is ongoing.

- Privacy policies are unique to the environment; thus, best practices have yet to follow.
- Building consensus on privacy policies takes time.
- The consumer role in privacy policy development is limited.

HIPAA was not the first effort by government to assure the public that the privacy of an individual's medical information would be secure. The Privacy Act of 1974 established key provisions to protect the privacy of patients (CMS 2005e). Enacted before the conception of electronic health records prevalent today, the legislation protected all patient records with "personal identifiers" (social security number or other). Under the Privacy Act, every patient can access and, if necessary, correct his or her individual records, and it generally prohibits disclosure of these records—but that applied only to federal agencies.

The individual's right to genetic privacy was also addressed in Oregon's Genetic Privacy Act of 1995, which provides legal protection for medical information, tissue samples, and DNA samples. Harris and Keywood (2001, 415) pointed out that individuals "have a powerful interest in genetic privacy and its associated claim to ignorance"; however, "any claims to be shielded from information about the self must compete on equal terms with claims based in the rights and interests of others." Further, Cummings and Magnusson (2001, 1089) stated that "As genetic privacy legislation is developed and enacted at state and federal levels, the needs of individuals must be balanced with the needs of institutions and of research in the larger context of societal needs."

Now, the Patient Protection and Affordable Care Act of 2010 has increased the rigor of the HIPAA rules further by requiring a unique Health Plan Identifier and both standards and rules for financial transactions.

Health Information Technology for Economic and Clinical Health Act

President Obama signed the American Recovery and Reinvestment Act (ARRA) in February 2009. This comprehensive stimulus package is designed to address the 2007–2009 economic crisis. ARRA contains many provisions, including tax relief (federal); unemployment benefit expansion; social welfare spending; and spending for specific sectors such as energy, education, and healthcare. The healthcare spending is diverse, allocating funds or subsidies for Medicaid, health research and construction, benefits for the newly uninsured, prevention and wellness, and research on the effectiveness of healthcare treatments, among many other provisions.

A major part of ARRA is called the Health Information Technology for Economic and Clinical Health (HITECH) Act. It is designed to promote

the expansion of the electronic health record (EHR) because of its perceived social benefits. A total of about $22 billion was allocated to the HITECH Act, with the bulk ($19.2 billion) devoted directly to EHR adoption. An additional $2 billion went to the Office of the National Coordinator for Health Information Technology (ONCHIT 2011) to support the agency's varied activities for promoting information exchange, training health professionals for information technology, and enhancing interoperability. ONCHIT is the body responsible for implementing the incentives for EHR use and establishing an HIT Policy Committee and an HIT Standards Committee. These committees are charged with developing recommendations for adopting health information infrastructure and standards for information exchange, respectively (Recovery.gov n.d.).

Adoption of EHR

From a broad social perspective and consistent with our earlier justification for government intervention, the benefits of the meaningful use of EHRs include the following, as identified by HealthIT.gov (n.d.):

- Complete and accurate information
- Better access to information
- Patient empowerment

One can argue whether the government or private sector is better at realizing these goals, but some opine that the benefits of sharable electronic information accrue to society at large and thus cannot be fully captured by any private provider or organization. Consequently, investing in this public good can be justified.

Meaningful Use

The HITECH Act provides the authority to make changes that can improve healthcare quality, safety, and efficiency through the use of EHR and the exchange of electronic health information. ONCHIT has released regulations to define appropriate standards for the certification of EHR technologies and the means by which providers can receive financial incentives to adopt and use those systems (see www.healthit.gov/policy-researchers-implementers/about-certification). An example of one of the many features of the HITECH Act is the meaningful use provision, which offers incentives to organizations that adopt and implement EHRs. The underlying assumption is that EHRs can provide benefits to providers and patients. The benefits may not be realized, however, without sufficient intensity of use. Consequently, CMS developed a set of standards called *meaningful use*. These standards allow hospitals and individual providers deemed eligible to obtain incentive

payments by meeting specific criteria; the incentives for adoption by clinical professionals are substantial, as seen in Exhibit 3.6.

For professionals applying in 2011, the maximum payment was $44,000 over the period. Notice the built-in incentives to begin the process early: The initial payment was lower for eligible professionals who delayed EHR. Eligible professionals for Medicare's incentive program include doctors of medicine, osteopathy, dentistry, podiatry, optometry, and chiropractic medicine. For Medicaid, the professionals who may participate include nurse practitioners, certified nurse midwifes, and select physician assistants. Hospitals eligible for participation in Medicare incentives include those receiving inpatient prospective payment, critical access hospitals, and Medicare

EXHIBIT 3.6 CMS Meaningful Use Incentive Payment Schedule for Medicare-Eligible Professionals

Payment Amounts	If a Medicare-Eligible Professional Qualifies to Receive First Payment in 2011	If a Medicare-Eligible Professional Qualifies to Receive First Payment in 2012	If a Medicare-Eligible Professional Qualifies to Receive First Payment in 2013	If a Medicare-Eligible Professional Qualifies to Receive First Payment in 2014	If a Medicare-Eligible Professional Qualifies to Receive First Payment in 2015
Payment amount for 2011	$18,000				
Payment amount for 2012	$12,000	$18,000			
Payment amount for 2013	$8,000	$12,000	$15,000		
Payment amount for 2014	$4,000	$8,000	$12,000	$12,000	
Payment amount for 2015	$2,000	$4,000	$8,000	$8,000	
Payment amount for 2016		$2,000	$4,000	$4,000	
Total Payment Amount	$44,000	$44,000	$39,000	$24,000	

SOURCE: CMS (n.d.[a], 2010b).

Advantage hospitals. Medicaid qualifications include inpatient hospitals with 10 percent Medicaid patient volume or any children's hospital.

The catch in EHR incentive participation is that the level of use must be deemed "meaningful." Incentive payments come in three stages. Stage 1 (implemented in the 2011–2012 period) involves installing certified information systems that capture structured patient data and give the ability to share that data with the patient or other healthcare professionals. Stage 2 (scheduled for 2014) requires more collection and reporting to advance clinical processes. Stage 3 (scheduled for 2016) requires actual improved outcomes. The HIT requirement for meaningful use is clearly detailed in Stage 1. Eligible providers must report providing all 15 Core Measures, a choice of 5 out of 10 menu objectives, and 6 clinical quality measures. The 15 Core Measures are listed in Exhibit 3.7. Each of the core measures has detailed definitions and reporting requirements. Consult this government publication for the specifications: www.cms.gov/EHRIncentivePrograms/Downloads/EP-MU-TOC.pdf. As an example, the following is the specification for the measure computerized physician order entry (CPOE):

> Requirement: More than 30 percent of unique patients with at least one medication in the medication list and seen by the eligible professional must have at least one medication entered using CPOE. You can be excluded from this core measure if you write fewer than 100 prescriptions during the reporting period.

EXHIBIT 3.7 15 Core Measures for CMS Meaningful Use Standards for Eligible Professionals

1. Implement computerized physician order entry
2. Perform drug–drug and drug–allergy checks
3. Maintain up-to-date problem list of current and active diagnoses
4. Use e-prescribing (eRx)
5. Maintain active medication list
6. Maintain active medication allergy list
7. Record demographics
8. Record and chart changes in vital signs
9. Record smoking status for patients aged 13 or older
10. Report ambulatory clinical quality measures to CMS/states
11. Implement clinical decision support
12. Provide patients with an electronic copy of their health information, upon request
13. Provide clinical summaries for patients for each office visit
14. Establish capability to exchange key clinical information
15. Protect electronic health information

SOURCE: CMS (2010a).

The ten menu objectives (see Exhibit 3.8) are also required, and their specifications are found on the website mentioned earlier. While this list of objectives gives you some choice, the first two are public health–oriented and thus one of the two must be selected. Basically, meaningful use demands that providers demonstrate that they can effectively communicate population-based information from their practice.

Eligible professionals also must report six clinical quality measures. Three of the six are core, and the three others can be selected from a large list of measures (see Exhibit 3.9). The three primary and three alternate core measures (which are available should the primary measures not apply to the provider's patient population) include the following:

- Primary measures
  - Hypertension: Blood pressure measurement
  - Preventive care and screening: Tobacco use assessment and tobacco cessation intervention
  - Adult weight screening and follow-up
- Alternate measures
  - Weight assessment and counseling for children and adolescents
  - Preventive care and screening: Influenza immunization for patients aged 50 or older
  - Childhood immunization status

The remaining three quality measures must be selected from the 38 measures listed in Exhibit 3.9.

EXHIBIT 3.8
10 Menu Objectives for CMS Meaningful Use Standards

1. Submit electronic data to immunization registries
2. Submit electronic syndromic surveillance data to public health agencies
3. Perform drug formulary checks
4. Incorporate clinical lab-test results
5. Generate lists of patients by specific conditions
6. Send reminders to patients for preventive/follow-up care
7. Provide patient-specific education resources
8. Provide electronic access to health information for patients
9. Perform medication reconciliation
10. Maintain summary-of-care record for transitions of care

SOURCE: CMS (2010a).

The set of reporting requirements that apply to eligible hospitals includes 14 core measures, 5 of 10 menu objectives, and 15 quality measures. Details on these items are found in the following documents posted on the CMS website (www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Meaningful_Use.html):

- ALL Stage 1 EHR Meaningful Use Specification Sheets for Eligible Hospitals
- Hospital Attestation Worksheet
- Critical Access Hospital Payment Tip Sheet
- EHR Incentive Program for Medicare Hospitals
- EHR Incentive Program for Critical Access Hospitals—Spanish Version
- Medicaid Hospital Incentive Payments Calculations

We have only discussed Stage 1 of meaningful use. Stages 2 and 3 are on the books but are not yet fully developed, and Stage 2 meaningful use core and menu measures were not released until October 2012 and are not scheduled to be implemented until fiscal year 2014. Those working with HIT *must* know where to go for the latest information, as these requirements are updated and revised occasionally. This website offers relevant information: www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Stage_2.html.

The evidence of the impact of EHR adoption for hospitals and physicians is disappointing, despite the financial incentives and emphasis. Davis (2009) reports, using detailed HIMSS Analytics databases, that by 2008 few hospitals had attained any of the top four levels of adoption. Only 5.8 percent of respondents reported implementing CPOE and clinical decision support

EXHIBIT 3.9
Clinical Quality Measures for CMS Meaningful Use Standards

1. Diabetes: Hemoglobin A1c poor control
2. Diabetes: Low-density lipoprotein (LDL) management and control
3. Diabetes: Blood pressure management
4. Heart failure (HF): Angiotensin-converting enzyme (ACE) inhibitor or angiotensin receptor blocker (ARB) therapy for left ventricular systolic dysfunction (LVSD)
5. Coronary artery disease (CAD): Beta-blocker therapy for CAD patients with prior myocardial infarction (MI)
6. Pneumonia vaccination status for older adults
7. Breast cancer screening
8. Colorectal cancer screening

(*continued*)

EXHIBIT 3.9 Clinical Quality Measures for CMS Meaningful Use Standards (*continued*)

9. Coronary artery disease (CAD): Oral antiplatelet therapy prescribed for patients with CAD
10. Heart failure (HF): Beta-blocker therapy for LVSD
11. Antidepressant medication management: (a) effective acute phase treatment, (b) effective continuation phase treatment
12. Primary open angle glaucoma (POAG): Optic nerve evaluation
13. Diabetic retinopathy: Documentation of presence or absence of macular edema and level of severity of retinopathy
14. Diabetic retinopathy: Communication with the physician managing ongoing diabetes care
15. Asthma pharmacologic therapy
16. Asthma assessment
17. Appropriate testing for children with pharyngitis
18. Oncology breast cancer: Hormonal therapy for stage IC-IIIC estrogen receptor/progesterone receptor (ER/PR) positive breast cancer
19. Oncology colon cancer: Chemotherapy for stage III colon cancer patients
20. Prostate cancer: Avoidance of overuse of bone scan for staging low-risk prostate cancer patients
21. Smoking and tobacco use cessation, medical assistance:
    (a) Advising smokers and tobacco users to quit
    (b) Discussing smoking and tobacco use cessation medications
    (c) Discussing smoking and tobacco use cessation strategies
22. Diabetes: Eye exam
23. Diabetes: Urine screening
24. Diabetes: Foot exam
25. Coronary artery disease (CAD): Drug therapy for lowering LDL cholesterol
26. Heart failure (HF): Warfarin therapy patients with atrial fibrillation
27. Ischemic vascular disease (IVD): Blood pressure management
28. Ischemic vascular disease (IVD): Use of aspirin or another antithrombotic
29. Initiation and engagement of alcohol and other drug-dependence treatment: (a) initiation, (b) engagement
30. Prenatal care: Screening for human immunodeficiency virus (HIV)
31. Prenatal care: Anti-D immune globulin
32. Controlling high blood pressure
33. Cervical cancer screening
34. Chlamydia screening for women
35. Use of appropriate medications for asthma
36. Low back pain: Use of imaging studies
37. Ischemic vascular disease (IVD): Complete lipid panel and LDL control
38. Diabetes: Hemoglobin A1c control (<8.0%)

SOURCE: CMS (2010a).

systems, which are level 4 or higher. Nearly 16 percent of respondents had not yet installed laboratory information systems, pharmacy information systems, or radiology information systems, which are the minimum necessary to advance from the bottom level of EHR adoption. Davis concluded that for hospitals to meet meaningful use criteria by 2013, they had to have reached at least level 4. The numbers for physicians were equally discouraging. EHR adoption in US hospitals and physician practices lags in comparison with adoption rates in other industrialized countries (Jha et al. 2008).

Patient Protection and Affordable Care Act

No single legislation in the past several years represents the government's attempt to address a host of social problems in healthcare more than the Patient Protection and Affordable Care Act. Signed on March 23, 2010, HR 3590 and the accompanying HR 4872 (Health Care and Education Reconciliation Act of 2010) proposed historic changes to the US healthcare delivery and financing system. Designed to expand coverage, the ACA contains a host of provisions with short-term and far-reaching implications. Due to its size, however, most individuals tend to focus on issues of importance to them only. For example, the American Hospital Association (2010) released a summary highlighting eight key features of the legislation important to AHA's constituents:

1. Coverage: expansion of insurance to more than 30 million Americans
2. Delivery system reforms: changes in incentives facing providers to enhance quality, reduce costs, and improve care coordination; this section has the accountable care organization authorization
3. Medicare and Medicaid payment: efforts to reduce the rate of increased spending on these programs, with hospitals being the major target; provisions for a drug discount program, payments to rural hospitals, and enhancements to primary care physicians are also included here
4. Workforce and graduate medical education: expansion and alteration of workforce training to alleviate the shortages in select portions of the healthcare workforce
5. Wellness and prevention: allocation of resources to the Prevention and Public Health Fund and insurer requirement to cover immunizations and screenings with zero cost sharing
6. Quality, disparities, and comparative effectiveness: begins the movement to pay for quality and penalties for hospital-acquired conditions
7. Regulatory oversight: provisions to identify and reduce fraud and abuse, including the continuation of the RAC audits
8. Revenue: to pay for much of these features, the law taxes high cost health insurance plans and imposes fees on select industries

Many of the ACA features cause stress for HIT, but the following deserve special mention. First, accountable care organizations (ACOs) assign responsibility (accountability) to the organization for patients who may not obtain all or even most of their care from the host organization (Kaiser 2012; Miller 2009). Finding the patient, effectively exchanging information with other providers, and ensuring the privacy and confidentiality of that information outside of organizational boundaries are a challenge. That information is exchanged both ways, so even if the institution is not sponsoring an ACO, it may be asked to provide clinical information on select patients.

Second, pay-for-performance initiatives demand greater linkages between provider cost and clinical performance than is customary (Rosenthal and Dudley 2007; Rosenthal and Camillus 2007). The discussion in Chapter 4, regarding management across organizational boundaries, is put to the test as clinical (chief medical officers and chief nursing officers) and financial (chief financial officers) leaders demand accurate and timely data for evaluation, improvement, and contracting purposes.

Third, expansion of covered lives is taxing to HIT in a number of ways. Having more patients can be a minor stressor, but (depending on current capacity) sufficient volume growth might require added facilities. In addition, at least some new patients are likely to be unfamiliar with the delivery system and thus less compliant with completing forms and documentations necessary to manage the care process. Further, some added patients may be "sicker" and may present new problems to the clinicians, testing the provider's documentation, coding quality, and select systems in unforeseen ways.

Fourth, as Gawande (2010) pointed out, there is a host of pushback efforts to the ACA as there was to Medicare and Medicaid decades before, which emphasizes Gawande's argument that "the battle for health-care reform has only begun." More than any individual ACA feature causing concern for HIT leadership is that the timing of implementation is highly uncertain. Planning for an unknown future makes life difficult for HIT management, but that may justify the salary that HIT leadership receives.

HIT Leadership Roles

While government involvement through HIPAA, the HITECH Act, and the ACA may seem difficult for information technology specialists to fully understand, it is particularly baffling for those outside of HIT. The consequence of this difficulty is that it requires HIT leadership (chief information officer [CIO] and others) to understand, anticipate, and explain the impact of these legislations. They must be prepared for new and/or changes in government

regulations and policies by developing and then implementing a number of activities and programs, including comprehensive environmental scanning and organizational education, information security policies and procedures, disaster preparedness and recovery planning, and information privacy and confidentiality protection.

Environmental Scanning and Organizational Education

The first responsibility of HIT leadership is to fully understand the operational and resource implications of all legislations. Internally, the team must understand what it has to do differently as a result and determine what extra staffing, expertise (consultants), hardware and software, and time are needed. The steps for this activity are as follows:

1. Determine breadth and scope of impending or current legislation.
2. Assess current organizational readiness for the impact.
3. Perform a gap analysis within the organization.
4. Recommend strategies to meet legal/regulatory changes.
    a. Develop staffing and critical expertise needed to address changes:
    b. Specify hardware and software needs.
    c. Estimate total financial implications of the recommendations.
5. Identify clinical and other resources within the organization that are necessary in meeting the standards.
6. Outline a timeline for implementation with key dates and milestones.

Naturally, difficulty may be encountered in effectively accomplishing these tasks once the legislation is in place and the deadlines are looming. Consequently, HIT leadership should be constantly monitoring the horizon for proposed legislation to get a head start on planning for its passage. To do this, HIT leadership should be engaged with those responsible for legislative affairs within the organization (if such a role exists). Getting a "heads up" from this source is vital. State and national associations—such as the Healthcare Information and Management Systems Society, American College of Healthcare Executives, Healthcare Financial Management Association, and American Hospital Association, among many others—are good sources of this "pre" data. A body of literature is available as well that documents the many and varied impacts of HIPAA, the HITECH Act, and the ACA. It is important for HIT leadership, either directly or through surrogates, to monitor and stay up-to-date on this literature. For example, Houser, Houser, and Shewchuk (2007) use the nominal group technique (NGT) for gathering information regarding the impact of HIPAA privacy rules on the release of patient information. "The NGT approach is a consumer-oriented formal brainstorming or idea-generating technique that is assumed to foster

creativity and to be particularly effective in helping group members articulate meaningful disclosures in response to specific questions" (Houser, Houser, and Shewchuk 2007, 2).

Because the nature of government legislation, such as HIPAA, can be highly complex, HIT leadership should be prepared to educate senior leadership on the implications of these regulatory interventions. Senior leadership includes the chief executive officer as well as the chief operating officer (if the organization has that position), chief medical officer, chief nursing officer, and chief financial officer. Generally, the person responsible for strategic planning, the head of the legal department, the head of human resources, and the head of development should be educated also in HIT-related legislative matters.

Information Security Policies and Procedures

Healthcare organizations must establish enterprisewide standards to maintain data security and protect the privacy and confidentiality of information, particularly patient records. Data security involves two essential elements: (1) protecting against system failures or external catastrophic events, such as fires, storms, deliberate sabotage, and other destructive acts of man and nature that could result in critical information being lost, and (2) controlling access to computer files by unauthorized personnel.

Disaster Preparedness and Recovery Planning

The HIT steering committee must ensure that effective data backup and recovery procedures are implemented at all processing sites throughout the organization. Critical data files should be copied to removable disk packs or tapes and stored in a secure location away from the processing sites, preferably in a different building. The CIO should develop a data backup plan for approval by the steering committee. The plan should specify which files require duplication and how often backup procedures should be conducted. Recovery procedures to be used if catastrophic events occur should also be included.

The need for disaster planning was underscored by the terrorist attacks in New York City on September 11, 2001. If that event was not convincing, Hurricane Katrina and the resulting challenges surely were. Disaster plans must be implemented, tested periodically, and refined. Testing of the plan provides training for employees and helps identify shortcomings in technology and procedures before they need to be used. A disaster-plan notebook should be developed and stored at the healthcare facility, at an off-site storage location, and at the homes of key employees who are involved in recovery procedures (Vecchio 2000).

Consultants can be used to assist in disaster planning and recovery. For example, IRM International offers a disaster recovery program that includes four phases: assessment, documentation consolidation, disaster plan development, and testing and refinement. See www.irminternational.com/rptcard.html for a disaster recovery report card that rates disaster-planning readiness.

In addition, data can be lost through computer viruses, which are increasingly prevalent and destructive. Each computer program should be inspected by virus-protection software every time the program is run. Acquisition of software should be subject to central review and approval, and particular care must be exercised to ensure that software downloaded from the Internet or obtained over networks is scanned and proven to be virus free. All incoming e-mail messages should be scanned for viruses, and employees should be trained not to open suspicious files attached to an e-mail, text, or any other electronic communication.

Information Privacy and Confidentiality Protection

As suggested in the earlier discussion related to HIPAA, the HITECH Act, and the ACA, protecting information privacy and confidentiality should be a major concern of the HIT leadership. A comprehensive information security policy should include three elements: (1) physical security, (2) technical controls over access, and (3) management policies that are well known and enforced in all organizational units (Stahl 2003) (see Exhibit 3.10).

Understanding the processes of information privacy and confidentiality is not a necessary step to successful implementation at the systems level. While the past decade offers many examples of how individual systems have accomplished these goals, evidence indicates that many organizations are still not compliant with basic security standards (Davis and Having 2006). Some in the healthcare field have called for systematic incentives from industry or insurers to induce organizations to adopt privacy and security technology (e.g., Lang 2006). Despite substantial improvements, however, violations of basic privacy rights by hospitals and other providers are still a challenge (Hiltzik 2012). For an up-to-date list of privacy rule violations and settlements, see www.hhs.gov/ocr/office/news/index.html.

Physical Security	Technical Safeguards	Management Policies
Hardware	Passwords	Written security policy
Data files	Encryption	Employee training
	Audit logs	Disciplinary actions for violations

EXHIBIT 3.10 Components of Information Security

Prior to implementation of HIPAA standards, the Mayo Clinic, based in Rochester, Minnesota, developed a comprehensive set of plans to keep electronic medical records secure. A multidisciplinary team formulated the policy and provided management oversight of the security program. Leaders of the Mayo Clinic effort suggested that a confidentiality policy should include the following elements (Olson, Peters, and Stewart 1998, 29):

- Access rights—who has access and for what reasons
- Release of information to the patient, other healthcare providers, and third parties
- Special handling, if any, for specific information (e.g., HIV results, psychiatric notes)
- Special handling, if any, for particular patients (e.g., employees or VIPs)
- Availability of medical information, including retention policies
- Integrity of medical information, including authentication, completeness, and handling of revisions or addenda
- Approved methods for communication of medical information

Summary

This chapter presents three major ideas. First, it presents and explores government's role in HIT. Government intervention in business processes can be justified if markets fail in their role of allocating scarce resources. Understanding why government gets involved assists healthcare and HIT leaders in responding to legislation and anticipating future actions. In healthcare, there are compelling reasons for government intervention, including a weak business case for information technology investment by providers, system fragmentation and lack of interoperability, and regulatory restrictions from fraud-and-abuse standards.

Second, the chapter explores specific legislations—HIPAA, the HITECH Act, and the ACA. These major government legislative and administrative interventions have fundamentally changed HIT. Passed by the US Congress in 1996, HIPAA—particularly two of its components—has a direct impact on healthcare information systems. The administrative simplification provisions of the law are designed to improve efficiency in the healthcare system by establishing uniform, national standards to be used for the electronic transmission of certain financial and administrative transactions. The privacy protection components of HIPAA restrict disclosure of health information

to the minimum needed for patient care and administrative support. Patients have gained new rights to access their medical records and to know who has accessed them. HIPAA compliance requires that most healthcare organizations and their software vendors make modifications to computer software to meet the data standards and privacy protection provisions of the law. Changes to business processes and procedures are needed as well. Education and training of employees is particularly important.

The HITECH Act, which is part of the American Recovery and Reinvestment Act of 2009, is designed to facilitate the transition of physicians, hospitals, and other healthcare providers to full users of EHR. Through Medicare and Medicaid reimbursement, the HITECH Act offers financial incentives for adoption and meaningful use of EHR. The HITECH Act established the Office of the National Coordinator for Health Information Technology to foster the electronic exchange and use of health information as well as to enforce health information privacy and security. The ACA is intended to decrease the number of uninsured by introducing incentives and insurance-coverage regulations for both employers and the general population. It also seeks to improve health outcomes and insurance eligibility by eliminating exclusions for preexisting conditions.

Healthcare information systems contain sensitive information. Policies and procedures are needed to protect the confidentiality of information about patients, employees, finances, and organizational strategies. This information is contained in patient care systems, public health systems, and medical research systems. While benefits of public health and medical research systems sometimes conflict with threats to individual privacy, federal and state governments have asserted that providers have a legal and moral obligation to protect patients' rights to privacy. Consequently, all of the laws passed at the federal, state, and local levels of government are aimed at protecting medical information privacy while improving the delivery and outcomes of care.

Finally, the chapter explores HIT leadership roles. The external environment and the government have direct, indirect, and substantial roles in healthcare operations. HIT leaders must understand those roles today and anticipate roles in the future. This section presents an action plan for HIT leadership. In response to HIPAA and other HIT-related legislations—and for ethical reasons as well—healthcare organizations and HIT leadership need enterprisewide standards and policies to maintain data security and protect the confidentiality of certain information. A comprehensive information security program requires disaster protection and recovery procedures as well as procedures for limiting access to certain information stored in computer databases.

Web Resources

A number of organizations (through their websites) provide more information on the topics discussed in this chapter:

- American National Standards Institute (www.ansi.org)
- Center for Democracy & Technology, Health Privacy (www.healthprivacy.org)
- Data Interchange Standards Association (www.disa.org)
- IRM International (www.irminternational.com/rptcard.html), a checklist for disaster recovery
- National Committee on Vital and Health Statistics (http://ncvhs.hhs.gov/index.htm)
- National Uniform Claim Committee (www.nucc.org)
- US Department of Health & Human Services:
  - Office of Civil Rights (www.hhs.gov/ocr/office/news/index.html) offers news releases announcing all of the major settlements of privacy and security breaches.
  - HealthCare.gov (www.healthcare.gov) provides information on evolving health insurance options available.
  - Centers for Medicare & Medicaid Services (www.cms.gov) points to detailed information about CMS's core programs and to research and data of value to HIT professionals. General HIPAA information can be found here: www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/index.html. Details of the EHR Incentive Programs are on www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html.
- Workgroup for Electronic Data Interchange (www.wedi.org)

Discussion Questions

1. Discuss the effects of government involvement in two other industries. Compare the differences and similarities of these industries with the healthcare field.
2. Discuss the impacts of a breach to healthcare information systems, especially the financial and privacy impacts.
3. What is HIPAA? Why was it passed? What are the potential benefits to healthcare organizations to be gained by compliance with HIPAA standards? What are the potential drawbacks?

4. What is the HITECH Act? Why was it passed? What are the potential benefits to healthcare organizations to be gained by responding to the Act's incentives? What are the potential drawbacks?
5. What is the ACA? Why was it passed? What are the potential benefits to healthcare organizations to be gained as ACA features become implemented? What are the potential threats from the ACA?
6. Discuss some of the potential conflicts between a patient's right to privacy and information needed for public health and medical research.
7. There are several implications to the use of provider and employer identification. Please discuss the positive and negative implications.
8. Why are the transaction and code set standards important? What is their value to healthcare?
9. What concepts are important to information security policies and procedures? What effect does HIPAA have on healthcare organizations' policies and procedures? Are there any other laws that may affect them?
10. What concepts are important to disaster recovery policies and procedures? What effect does HIPAA have on those policies and procedures? Are there any other laws that may affect them?
11. Is it important to an organization to have a workgroup that focuses on determining the effects of government legislation? Please discuss your rationale.
12. What components should be included in a plan for protecting information privacy and confidentiality?