CHAPTER

4

HEALTH INFORMATION TECHNOLOGY GOVERNANCE AND DECISION RIGHTS

Learning Objectives

1. Define *governance* as it applies to health information technology (HIT) and describe its primary purpose.
2. Summarize the five major components of HIT governance.
3. Explain why charter, representation and decision rights, and accountability are vital to a governance plan.
4. Explain why HIT strategic planning has become more important for healthcare organizations.
5. Describe the major elements of a healthcare organization's planning effort.
6. Assess the major elements of an HIT strategic plan.
7. Describe systems theory and explain why it is vital to HIT governance and planning.

Overview

The competitive advantage that successful health information technology (HIT) governance may bestow has become the center of much discussion and even some debate. Smaltz, Carpenter, and Saltz (2007) and Kloss (2015), among many others (Broadbent and Kitzis 2005; Glaser 2002; Weill and Ross 2004), conclude that effective governance and expanding decision rights, inherent in HIT leadership, are essential for organizational success. The discussion of what *governance* and *decision rights* mean and how these concepts have evolved in healthcare organizations is a major portion of this chapter. Such emphasis on governance does not imply that the more traditional HIT strategic planning is either unimportant or out of date. Planning is still vital and is an important part of HIT governance.

Today, more than in the past, successful HIT governance and planning must address challenges from outside HIT operations. Broad questions that need to be addressed include these: What is HIT governance? What does *data governance* mean? Who is involved in governance processes? How are

participants in governance processes held accountable? How does transparency in the organization influence governance? How does the governance model differ from historical HIT strategic planning? What changes must be made in organizations to transform HIT functions to a corporate asset?

This chapter first presents an overview of HIT governance with a key discussion of charter, representation, accountability, and strategic planning. It then outlines strategic planning in healthcare organizations from the perspective of an integrated governance model. Topics covered include organizing an HIT strategic planning effort, the importance of system integration, the basics of systems theory, and management control and decision support systems.

Background of Health Information Technology Governance

Information systems in many healthcare organizations evolved piecemeal, rather than from a carefully controlled planning process. Specific requirements for capturing, storing, and retrieving data when needed were developed on an ad hoc basis as new programs and services were added. As a result, the same data were captured repetitively, files were duplicated, and information was not always available when needed. Analysts recognized that if an HIT planning process was not in place, priorities for developing individual computer applications were often established by the exigencies of the moment.

The broader corporate perspective suggests that governance is the way in which owners and managers of an organization manage the *agency problem*—the fundamental conflict of interest imposed by delegating operational authority to managers who do not own the resources managed (Denis 2001). Managers want to keep their job of running the business and thus may become risk averse in their decisions to minimize the chance that they will have a bad outcome that would cost them their employment. This risk aversion does not maximize returns to the owners. The owners want to make sure the business operates in such a way as to maximize its well-being, which means long-run profit in the business world and quality, reputation, or size for healthcare organizations. In any event, the challenge facing the owners or the governing board is how best to ensure that management makes the right decisions. Two solutions to this agency problem are bonding and monitoring.

Bonding is developing contracts that reward managerial behavior that leads to positive outcomes or penalize managerial behavior that leads to negative outcomes; incentive-based compensation is one method of bonding.

Monitoring, on the other hand, refers to owners closely observing managerial behavior to ensure managers behave as desired. Both bonding and monitoring strategies have costs. The complexity of the HIT functions being managed are so great that monitoring has a minimal chance of being successful in today's HIT world. Likewise, the weak link between the activities of the HIT leaders and the outcomes that owners desire make bonding strategies questionable. These strategies are made even more problematic during periods of rapid change. Specifying contracts and monitoring activity pose challenges in a changing environment.

HIT priorities have changed to focus on integration of systems across multiple facilities, automation of patient records, and improved decision support for clinicians and managers. Achieving these complex objectives requires a careful planning process to develop a functional, scalable, and flexible information architecture that facilitates data exchange and provides users real-time, remote access to information from any location.

This chapter covers three closely related topics that, while separate, must be considered together. First, we outline HIT governance with a discussion of purpose, then discuss governance for leadership, then present a governance plan. Second, we highlight how to organize an HIT strategic planning effort with some useful examples. Finally, we discuss system integration as a necessary component to governance and planning.

Purpose

HIT governance helps the organization make business decisions accurately and in a timely manner. With that benefit in mind, many have attempted to define the purpose and scope of HIT governance (e.g., Butler 2013; Data Governance Institute 2020a; Kloss 2015, 2013; Lutchen and Collins 2005; Sambamurthy and Zmud 1999; Weill and Ross 2004).

Haseley and Brucker (2012) present a compelling case for strict HIT governance review criteria. Following the IT Process Institute's guidelines, they propose five domains, or focus areas, that have meaning to all HIT processes (Haseley and Brucker 2012, 56):

> *Strategic alignment*—Maximize opportunities for the business use of IT while providing transparency and assurance that IT objectives are being achieved. This includes defining the IT value proposition, determining the linkage between business and IT plans and increasing managerial effectiveness.
>
> *Risk management*—Address legal and regulatory compliance needs and understand and manage key operation risks. This includes determining risk appetite and tolerance, assessing IT risk awareness and identifying risk exposures.
>
> *Resource management*—Appropriately align IT capabilities with business needs, including optimizing IT resources, optimizing knowledge and aligning capabilities.

Performance measurement—Utilize real-time data to continuously improve IT delivery. Approaches include measuring strategy implementation, reporting and the application of operational and strategic metrics.

Value delivery—Optimize return on IT investments by executing on the IT value proposition, meeting business requirements and verifying the integrity and accuracy of information.

Another, similar approach to purpose has been proposed in broad terms by Levy (2018). Differences mostly exist with regard to the level of granularity.

- *Ensure data availability.* The best systems with current technology are ineffective if the end users don't find the data easy to locate and use. Departments cannot own data; thus, governance must transcend the organization. In addition, with large, unstructured data storage, all users must understand what data are to be used and how best to process them. Availability requires that data schemes are applied consistently across organizational divisions.
- *Ensure consistency.* When leaders in your organization address problems using different data sets, they are likely to reach different conclusions. The resulting confusion and stress impede operational performance. All users must have access to consistent, reliable data, in order to facilitate valid comparisons and conclusions. Governance across the organization by a team of executives, managers, and data stewards with both the knowledge and vested authority ensure that all follow consistent rules.
- *Keep or delete data.* The risks of data hoarding are the same as those of physical hoarding. Servers and storage devices often fill up with unimportant, redundant, or just old data. This impedes the location of vital information and creates an opportunity for users to capture and use extraneous information. As much as one-third of the data stored is estimated to be unimportant. Often data not required for other reasons can be discarded quite quickly. Walmart uses only four weeks of transaction data, for example. Data governance provides rules for what must be kept and what can be discarded or archived.
- *Analyze and report issue resolution.* Effective organizational metrics and the data used to generate the metrics rely upon consistency across the organization. This includes recorded standards and definitions so that everyone understands the meaning from a common point. Business analytics provide useful information as long as they are fed the same data with the same definitions. Problems that arise are usually not the fault of the technology employed but misapplication of the tools and data used. Replacing basically sound systems will not solve the problem

but improved data governance can bring greater benefit, bring it much faster and at less cost.

- *Ensure security and compliance.* Consequences for noncompliance with data regulations can be enormous, especially where protected health information (PHI) from patients is concerned. Defining how its data are acquired, stored, backed up, and secured against accidents, theft, or misuse may enable the organization to avoid these consequences. Achieving secure data management and maintaining compliance with laws and regulations incorporates effective audits and controls to ensure that the procedures are followed. Beyond the formal control mechanisms, education and awareness campaigns will facilitate compliance with increasing user access to self-service solutions.

Governance for Leadership

The domains listed above from either scheme do not translate directly to the operational needs of HIT leadership. If you synthesize the information from Menning and Carpenter (2005); Smaltz, Carpenter, and Saltz (2007); and Herman, Scalzi, and Kropf (2011), you find the primary operational components of HIT governance necessary to achieve the key domains. These operational components are listed in exhibit 4.1 and discussed in more detail in the following sections.

Consistent (and Consistently Applied) Health Information Technology Strategy

HIT should support the strategic goals, objectives, and priorities of the organization it serves. As healthcare organizations have become more sophisticated, they use information more effectively to position themselves strategically in the environment where they operate (Austin, Trimm, and Sobczak 1995, 27; Shortliffe 2005).

As mentioned, hospitals and other healthcare organizations historically employed information technology (IT) to support day-to-day operations. Increasingly, healthcare managers are recognizing the role of information systems in increasing market share, supporting quality assessment and

1. Consistent (and consistently applied) HIT strategy
2. Alignment of HIT strategy with organizational strategy
3. Well-developed HIT infrastructure, architecture, and policies
4. Well-managed HIT project priorities and investments in HIT infrastructure
5. Documented HIT value or benefits to enhance accountability

EXHIBIT 4.1
Components of HIT Governance

improvement, and adding value to the organization. To accomplish these strategic objectives, the HIT plan must be consistently applied across the multiple operating units of an organization. Creating consistent applications in an environment that has grown piecemeal and that consists of employees who do not report directly to the chief information officer (CIO) presents a challenge.

HIT strategic planning has grown over the years, evolving into a field that has finally been given its due. In 1996, 35 percent of the respondents to the Healthcare Information and Management Systems Society's seventh annual leadership survey (HIMSS 1996) indicated that their organizations did not have an HIT strategic plan. By January 2002, that number went down, with only 8 percent of the responding organizations admitting that they lacked such a plan (HIMSS 2002). By 2005, the question of having an HIT strategic plan in place was left out of that year's survey and was replaced by a question of whether the plan was an integrated component of the organization's overall strategic plan (46 percent responded yes) or was integrated in content but stood as a separate plan (44 percent responded yes) (Scottsdale Institute and HIMSS Analytics 2005). In 2012, 48 percent of respondents to the 23rd annual survey indicated that their HIT strategic plan was a component of the organizational strategic plan, while 37 percent of respondents reported that the two plans were separate but integrated in content. Only 7 percent of respondents indicated that the HIT plan was not aligned, and 7 percent reported that the organization did not have an HIT strategic plan (HIMSS 2012, figure 19).

Planning is now a part of the culture for HIT. The question remains—Has the drive for consistency had an impact on how HIT priorities evolve? Only indirect evidence on this question exists, but if we consider HIMSS survey data for 2018, priorities remain relatively consistent for hospital IT respondents from 2017 to 2018 (HIMSS 2018, table 6). While some change occurred, the top priority remained the same in both years (patient safety). The second priority in 2018 (privacy, security, and cybersecurity) was third in 2017, and the fifth priority in 2018 (process improvement, workflow, and change management) was also fifth in 2017. The second priority in 2017 (electronic health records [EHRs]) fell to eighth place in 2018, and the fourth priority in 2018 (data analytics and clinical and business intelligence) rose from ninth in 2017. The decline in the EHR's priority ranking was probably a result of progress in improving these technologies by system vendors. Likewise, data analytics and clinical and business intelligence have been made more acute as evolving technologies open new opportunities.

The vendor or consultant portion of that same survey (HIMSS 2018, table 7) reveals similar consistency over this short time. Interestingly, the top priority for 2018, data analytics and clinical and business intelligence, was

ninth in 2017, reflecting the rise in opportunities for this application. Others in the top five were consistent, however.

Alignment of Health Information Technology Strategy with Organizational Strategy

The HIT strategic plan must be closely aligned with the strategic plan of the organization. The issue of alignment has been an integral part of the HIT planning mantra for years (see Ward and Griffiths 1996). Aligning HIT strategy with the overall organizational strategy requires (1) a consistently applied HIT plan and (2) the recognition by HIT leadership of the importance of the interrelationships among HIT, the rest of the organization, and the external environment. Moreover, Stacey and Skinner (2005) argue that alignment involves three essential elements for success. First, an alignment of purpose must be in place. HIT leadership and organizational leadership must agree that they are trying to achieve the same ends. Second, both sets of leaders must agree to work jointly to develop goals and tactics to meet those ends. Third, they must agree to share the responsibility and accountability for achieving the ends. In the words of Stacey and Skinner (2005, 41), "We're in this together." These references may be dated, but looking at more recent work (*Healthcare Business & Technology* 2017) reveals that the core points continue to apply.

Because business objectives change over time, the HIT plan should be reviewed frequently to ensure it remains in alignment with current organizational strategy. Implementing an aligned plan is much more difficult than stating the need for alignment. To assist leaders in achieving strategic alignment, the following six questions must be addressed by the CIO and organizational leadership together from the perspective of the organization:

1. What does the organization do?
2. Whom does the organization do it to or for?
3. Where does the organization do it?
4. When does the organization do it?
5. Why does the organization do it?
6. How does the organization do it?

Well-Developed Health Information Technology Infrastructure, Architecture, and Policies

Healthcare organizations must make choices and set priorities for their information systems. The plan should identify the major types of information required to support strategic objectives and establish priorities for installation of specific computer applications, the architecture on which the systems function, and the detailed rules that drive HIT operations.

To meet strategic objectives and develop high-priority applications, the healthcare organization must develop blueprints for its HIT infrastructure. This process involves making decisions about hardware configuration (architecture), network communications, degree of centralization or decentralization of computing facilities, and types of computer software required to support the network.

HIMSS attempts to determine current and future HIT use and adoption through its annual leadership surveys. Although the wording of survey questions evolves over time, they are similar enough to note the following shifts in focus since 2000:

- Early 2000s: system connectivity is key
  - High-speed networks
  - Intranets
  - Wireless information systems
  - Client and server systems
- 2012: infrastructure emerges as a top priority
  - Servers and virtual servers
  - Mobile devices
  - Desktops and virtual desktops
  - Security systems
  - Storage and backup
  - Wired and wireless networks
  - Cloud computing
  - Telemedicine
- 2018: system utility and applications take the forefront
  - Patient safety
  - Privacy security and cybersecurity
  - Process improvement and workflow
  - Data analytics and clinical and business intelligence
  - Clinical informatics and clinical engagement

The update for 2018 (HIMSS 2018) revealed some additional changes in priorities for hospitals. The focus of the survey changed slightly, addressing the question, What are your top priorities? Please note that framing of the question differed from prior years, so outcomes are less comparable over time. Interestingly, the same question was asked of vendors and consultants, revealing the differing focus of the two groups:

- Data analytics and clinical and business intelligence
- Health information exchange, interoperability, and data integration
- Improving quality outcomes through HIT
- Privacy security and cyber security
- EHRs

After the infrastructure and architecture are developed, the HIT steering committee (see the section titled Organizing Health Information Technology Strategic Planning Effort) should oversee the development of a set of enterprise-wide policies that govern the design, acquisition, and operation of information systems throughout the organization. Important policies needed by every organization include data security policies; data definition standards; policies governing the acquisition of hardware, software, and telecommunications network equipment; and policies on use of the internet.

Data Standardization

As discussed, system integration is an important element of HIT strategic planning in healthcare organizations. Most computer applications must include the ability to share information with other systems. This requirement has come to the attention of many operations and research organizations in healthcare (Observational Health Data Sciences and Informatics 2020). For example, a laboratory results reporting system must be able to transfer information for storage to the EHR. Electronic data exchange cannot occur without some level of standardization of data structures. For this reason, healthcare organizations should consider developing a *data dictionary*—a tool or list that specifies or defines the format of each data element and the coding system (if any) associated with that element. For example, the data dictionary might define the data element "date of birth" as follows:

> Date of birth—Eight-digit numeric field with three subfields:
> Month—two digits ranging from 01 to 12
> Day—two digits ranging from 01 to 31
> Year—four digits ranging from 1850 to 2100

In this example, notice that the range of the subfield for year is designed to accommodate historical records of patients with birth dates that go backward to the mid-nineteenth century and forward to the end of the twenty-first century.

In addition to data compatibility among information systems within the organization, there is a growing need to facilitate the exchange of

information among health systems, government and private insurance companies, medical supply and equipment vendors, and other entities. A number of projects have been initiated to develop voluntary, industry-wide standards for electronic data interchange in the healthcare field. Examples of these projects include the following:

- The American National Standards Institute (ANSI; www.ansi.org) X.12 Group works on specifications for transactions involving the processing of health insurance claims.
- The Health Industry Business Communication Council (www.hibcc.org/about-hibcc/overview) works to provide common coding of supplies, materials, and equipment.
- Health Level Seven (HL7, version 3; www.hl7.org) is a standard for healthcare electronic data transmission. It is now marketed as HL7 International.
- The Healthcare Information Technology Standards Panel (HITSP; www.hitsp.org) received a contract from the US Department of Health & Human Services (HHS) to support a new collaborative effort to harmonize HIT standards.

The HL7 project, initiated in 1987, is a voluntary effort by healthcare providers, hardware and software vendors, payers, consultants, government groups, and professional organizations. The broad goal is developing a cost-effective approach to system connectivity by developing standards for clinical and administrative data. As with other standards-developing organizations certified by ANSI, HL7 develops messaging specifications that enable organizations to exchange clinical and administrative data; it has been working on improving these specifications since 1987. Version 3 of HL7 embodies a new approach that addresses many of the weaknesses of earlier versions and encompasses messaging, component specifications, structured document architecture, and more. Even earlier versions provided a coherent set of standards for messages, component interfaces, and documents that all users can embrace (Beeler 2001). The technology and applications update continuously and expand in scale and scope (Levin 2019).

The federal government has continued to support the creation and adoption of HL7 and other data exchange standards. As a part of the presidential initiative on consolidated health informatics, HHS and the departments of Defense and Veterans Affairs announced the adoption of HL7 messaging standards along with prescription drug, imaging, and other standards in 2003 (georgewbush-whitehouse.gov 2020). These standards enable

the federal agencies to share information and improve coordination of care. Similarly, in 2004, five additional standards related to information exchange were announced (georgewbush-whitehouse.gov 2020).

In addition to these voluntary efforts at industry-wide data standardization are the mandatory electronic data standards and standard transaction formats for claims processing, which were established by the Health Insurance Portability and Accountability Act (HIPAA) of 1996. Providers are required to follow these standards to receive reimbursement from Medicare, Medicaid, and other health insurers. As a means of addressing growing mandatory standards, "HITSP [brings] together a wide range of stakeholders to identify, select, and harmonize standards for communicating data throughout the healthcare spectrum" (ANSI 2005). Under a contract from the Department of Health & Human Services and the sponsorship of ANSI, HIMSS, the Advanced Technology Institute, and Booz Allen Hamilton (a strategic partner), HITSP attempts "to accelerate the adoption of health information technology and the secure portability of health information across the United States" (AHRQ 2005). The purpose of HITSP is to develop a generally accepted "set of standards specifically to enable and support 'widespread interoperability, accurate use, access, privacy and security of shared health information'" (ANSI 2005).

HITSP is designed to function with public and private partnerships that have the potential to access much of the healthcare community. If successful in getting healthcare software developers and users to adopt these standards, it will buoy the Nationwide Health Information Network initiative for the United States called for by former President George W. Bush in Executive Order #13335, which established the Office of the National Coordinator for Health Information Technology (ONCHIT).

The challenge of achieving data standards to enable organizations to share data internally and externally is a work in progress. Mostly concerned with the external challenge, the ONCHIT has continually updated information regarding the status, requirements, and progress of health data standardization. The standards and technology sections of the Office of the National Coordinator (ONC) are a valuable starting point for keeping current (see www.healthit.gov/topic/standards-technology/health-it-standards). While constantly changing, common information initiatives include the following:

- Federal Health Architecture (www.healthit.gov/hitac/committees/health-information-technology-advisory-committee-hitac) seeks to coordinate data exchange and reporting requirements across federal agencies responsible for delivery and support of healthcare.

- Interoperability Portfolio (www.healthit.gov/topic/interoperability) is the central repository of current standards development and setting.
- Standards (www.healthit.gov/topic/standards-technology) works to ensure that a functional infrastructure is in place to support the adoption of HIT throughout the country.
  - Scientific Initiatives (www.healthit.gov/topic/scientific-initiatives) leverages scientific information to support biomedical and health services research.
  - Usability and Provider Burden (www.healthit.gov/topic/usability-and-provider-burden) works to ease the burden of use by both patients and providers as technology has become pervasive.
- International Health IT Collaborations (www.healthit.gov/topic/international-health-it-collaborations) aims to assemble the planning and coordination being done with providers and systems abroad so that US HIT standards are not at odds or incompatible with HIT systems from other countries.

Despite these ongoing efforts, data standards still present major challenges. Panangala and Jansen (2013) published an assessment of the potential for the Department of Defense and the Veterans Health Administration to merge health information across active service and retired service member systems. They suggest that significant challenges exist; currently, the original goal of creating a single medical record for all service-connected personnel is being replaced by improved interoperability between the systems. Furthermore, health information exchanges (HIEs) are not progressing as quickly or easily as hoped (Kellerman and Jones 2013). HIE has not been stalled exclusively because of data standards, but Kellerman and Jones's analysis indicates that a major impediment is the failure to specify a standard structure and format of data exchanged or the definition of the terms used.

As part of the HIT strategic planning process, the steering committee should study requirements for data interchange, including HIPAA mandates, and should develop a policy on data standardization for the organization. For example, many hospitals and integrated delivery systems (IDSs) are specifying that all software purchased from vendors must meet an industry standard protocol such as HL7.

Hardware and Software Standards

Healthcare organizations need to develop a number of technical policies related to information systems. Most of these are highly technical and should be drafted by the CIO or the director of information systems operations. However, the HIT steering committee should oversee the creation of a broad

set of policies related to the acquisition of computer hardware, software, and network communications equipment for the organization.

The steering committee must determine whether the organization will require central review and approval of all computer hardware and software purchases. Such items are often the budgetary authority of individual organizational units, but compelling reasons exist for central review and approval, regardless of cost, including the following five:

1. Central review and approval helps ensure compatibility with enterprise-wide data standards, such as HL7.
2. Central review and approval of personal computer purchases can ensure that data terminals and workstations use a common operating system, such as Windows.
3. Central review and purchasing of generalized software provides cost advantages through the acquisition of site licenses for multiple users of common packages (e.g., word processing, spreadsheets, database management).
4. Central review and approval ensures that hardware and software are of a type that can receive technical support and maintenance from the HIT staff.
5. Central review and approval can help prevent illegal use of unlicensed software in the organization.

In addition, the HIT steering committee should approve the network communications plan for the enterprise. A variety of network configurations are possible, and the network plan must be compatible with the overall HIT development plan for the organization.

Well-Managed Project Priorities and Investments in Infrastructure

The HIT function must also effectively oversee the purchase and implementation of HIT infrastructure consistent with the needs of the organization. The specialized knowledge and skills of HIT staff and the growing complexity of the underlying technology make this overseer role vital to the success of HIT operations. The use of technology has made information available and accessible to clinical and administrative staff across the organization, but the infrastructure on which software and other applications operate in the systems through which data are transmitted remains the domain of HIT. While end users are vital considerations in the priority-setting process, governance of HIT requires HIT leadership to manage effectively the priorities among alternative investment options (Menning and Carpenter 2005). This management includes items directly from the HIT strategic plan; for example, as outlined by Stacey and Skinner (2005, 44), a hospital had to change all of

its human resources, finance, patient accounting, and other support services information systems to enable integration with the rest of the health system and investments that arise episodically (a good example was Y2K considerations; see Wilson and McPherson [2002]).

Documented Health Information Technology Value or Benefits to Enhance Accountability

The final purpose of HIT strategic planning is to provide data for estimating the budget and resources required to meet the objectives and priorities established through the planning process. Planning is the basis for developing operating and capital budgets for HIT in the organization. The importance of this purpose has increased as CIOs report the need to obtain value from existing HIT (Glaser and Garets 2005) and the move from value preservation to value creation (Kark 2018). Turisco (2000, 13) called for value management in justifying HIT investments: "There is a growing demand for ensuring that . . . HIT investment practices and processes not only justify the large cash outlays, but track and realize the value. . . . Values can only be realized through measurable business changes supported by the business units."

The Center for Information Technology Leadership published a number of articles arguing that greater documentation of HIT value is essential (e.g., Johnston, Pan, and Middleton 2002). This "call to the field" identified three dimensions from which to derive HIT value: financial, clinical, and organizational. With this direction, a host of studies have emerged to address all or some of these dimensions (see Buntin et al. 2011; Encinosa and Bae 2011; Menachemi et al. 2006; Rahimi and Vimarlund 2007). Despite some success in specific applications such as decision support (Stenner, Chen, and Johnson 2020), the field has yet to demonstrate value in a consistent and significant manner (Rudin et al. 2014). The financial return on these investments is addressed in more detail in chapter 12.

The financial dimension is the most obvious source of value, consisting of cost reductions, revenue enhancements, and productivity gains. Clinical enhancements seek evidence of HIT's impact on service delivery (e.g., adherence to protocols) and clinical outcome indicators. Organizational enhancements include stakeholder satisfaction improvements and risk reduction. In all cases, Johnston, Pan, and Middleton's (2002, 1) fundamental point is that healthcare executives currently must rely on "anecdote, inference, and opinion to make critical HIT decisions." The evidence is still mixed, but some studies show the value of HIT when applied to specific technologies such as computerized physician order entry (CPOE) (e.g., Johnston et al. 2003; Koppel et al. 2005; Yu et al. 2009), clinical decision support (Stenner, Chen, and Johnson 2020), and information exchange and interoperability (e.g.,

Walker et al. 2005). In addition, positive results have been observed when applied in small group practices (Miller et al. 2005) and among primary care physicians (Pizziferri et al. 2005) and when tangible and intangible financial benefits are examined (Simon and Simon 2006). At this point, diverse research has not yet achieved a consensus on the financial or clinical value of HIT.

Governance Plan

Developing a governance plan for the organization is not an easy task. HIT professionals and executives would agree with the purpose, but getting support and engagement proves to be a challenge. Major efforts by respected organizations have struggled with this for years. The Data Governance Institute (2020a; 2020b) provides the structure for what follows, although others have contributed (Butler 2013; Kloss 2015, Kloss 2013). The Data Governance Institute website provides more details (www.datagovernance.com). It is a substantial resource with many important sources that will be used in this text. The site is divided into two parts: Data Governance Basics and the DGI Framework. Basics include an introduction to the process, definition of governance, goals and principles, governance and stewardship, quality roles and responsibilities, and a data governance glossary. The framework provides a comprehensive set of processes to follow to implement data governance.

Charter

A broad definition of HIT data governance is the place to start our discussion of charters. Healthcare data governance defines decision rights and accountabilities for all information-related processes. It uses established models that limit who can take what actions with what information, and when they can take that action, under what circumstances that action can be taken, and what methods can be employed in that action. Organizations need a plan for handling data in a consistent manner throughout the organization. The charter ensures safe handling, done in compliance with regulations, and enables the organization to derive maximum value from information to improve business performance. The charter requires a formalized set of goals, guiding principles, and benefits from the perspectives from someone outside of the organization.

Goals

Goals of data governance may vary but typically include the ability to do the following:

- Enable better decision-making
- Reduce operational friction

- Protect the needs of data stakeholders
- Train management and staff to adopt common approaches to data issues
- Build standard, repeatable processes
- Reduce costs and increase effectiveness through coordination of efforts
- Ensure transparency of processes (Data Governance Institute 2020d)

Guiding Principles

Organizations must establish the principles derived from their specific environment. Some organizations heavily consider the politics involved in data governance, while others focus on data ownership, adequately apportioned accountability, recognition of data stakeholders, assignment of data stewardship, and developing data standards. Data governance principles help stakeholders come together to resolve the types of data-related conflicts that are inherent in every organization. A typical list from the Data Governance Institute (2020d) includes the following:

- *Integrity.* Data governance participants will practice integrity with their dealings with each other; they will be truthful and forthcoming when discussing drivers, constraints, options, and impacts for data-related decisions. The key staff need to be fully trusted as handlers of organization information as they negotiate rules for data collection, reporting, and sharing among various stakeholders.
- *Transparency.* Data governance and stewardship processes will exhibit transparency; it should be clear to all participants and auditors how and when data-related decisions and controls were introduced into the processes. Transparency can be a difficult principle to handle because not everything can be fully transparent, but key representatives should be included for all major decisions.
- *Auditability.* Data-related decisions, processes, and controls subject to data governance will be auditable; they will be accompanied by documentation to support compliance-based and operational auditing requirements. Again, the balance must be between sufficient documentation for external and internal reviewers to follow versus too much time and energy expended for needless efforts. Full ability to audit process also supports the transparency principle.
- *Accountability.* Data governance will define accountabilities for cross-functional data-related decisions, processes, and controls. Finding data overview shortcomings will benefit the organization. It is likely that for some elements, no person or segment has established accountability

or, even more likely, several segments have redundant accountability. In either case, resolving this will improve data and operational management.

- *Stewardship.* Data governance will define accountabilities for stewardship activities that are the responsibilities of individual contributors, as well as accountabilities for groups of data stewards. Formally assigning someone responsibility enhances accountability.
- *Checks and balances.* Data governance will define accountabilities in a manner that introduces checks and balances between business and technology teams, as well as between those who create and collect information, those who manage it, those who use it, and those who introduce standards and compliance requirements. Conflicts and internal stress arise when competing users and functions vie for control of aspects of organizational data. The data governance function should manage these potentially significant challenges.
- *Standardization.* Data governance will introduce and support standardization of enterprise data. While not everything can or should be standardized, widespread standardization supports efficient and effective business, clinical, and IT projects.
- *Change management.* Data governance will support proactive and reactive change management activities for reference data values and the structure and use of master data and metadata. While managing data changes becomes central for the data governance function, if, when, and how that change occurs present a necessary function. Building in the process for that change will effectively smooth these functions over time.

These principles and others you might introduce for your particular environment help stakeholders unite to resolve inherent data-related conflicts in the organization. As you move forward, consider the importance of external or neutral viewpoints regarding your data governance efforts. Individuals who provide such feedback can help you modify your vision and develop approaches to the following:

- Developing a value statement
- Preparing a roadmap
- Planning and funding the function
- Designing the structure
- Deploying necessary resources
- Governing the process
- Monitoring, measuring, and reporting the outcomes.