Driving Compliance through Data Governance

Save to myBoK

by **Sandra Nunn** , MA, RHIA, CHP

Healthcare organizations increasingly struggle to manage huge volumes of e-mail, hundreds of thousands of documents on shared drives, and hundreds of source and feeder systems that pour data and records into EHR systems, data warehouses, and decision support systems. This has given new panache to the old idea that governing data and data management should be the cornerstone of information services management.

Data governance is the set of policies and procedures that determine the who, how, and why of data management within the organization. Strong data governance supports compliance and legal efforts by organizing data for retrieval and retention, especially over the long term.

Governing Enterprise Information

Data governance hasn't been lacking to date, of course. Within IS departments, data administrators have created a portfolio of policies and procedures around who owns what data, how data should be defined (e.g., required fields), what measures will be taken to ensure data integrity, who establishes access rights to the data, how long data or records must be retained, how to decommission the system, and how data in the system interact with other systems (i.e., interoperability issues).

Extensive work went into these policies and procedures, but in reality most of it has remained largely dormant until now. Emerging external legal and compliance pressures have pushed these initiatives, and the efforts to manage unstructured information (via content management systems), into the spotlight.

The governance of structured information such as coded data has a long history and well-established practices. It is much easier to control a stream of structured information created by educated professionals than it is to govern information (both structured and unstructured) created by thousands of people within an organization. True data governance at the enterprise level enters the picture here.

It is through data governance that information can be organized for long-term retrieval and retention. Effective data governance enables those charged with protecting their healthcare organizations to locate the data, documents, and records they will need to mount a proper defense against litigation, whether it comes from federal or state authorities or a personal attorney.

Unorganized and unmanaged electronic records form mountains of information that impede employee performance and create patient and legal risks when critical data or records cannot be found. Pinpointing the cost of data lacking integrity involves finding where the organization lost its way or made wrong decisions based on misinformation that may be traceable back to more than one point.

Although healthcare executives have applied the term governance to managing cash, employees, production plants, technological assets, and multiple other "hard" assets, they have only recently realized the need to manage information. Now there is a push to create formal governance structures with reporting and decision-making mechanisms to manage those invisible, but critical resources.

Efforts to apply data governance from the top down have largely been doomed from a lack of organizational interest in an initiative that seemed distant from "real" work such as installing electronic health record or electronic billing systems.

The politics around data governance have also created obstacles, such as agreeing on who owns what systems and what accountabilities ride along with that ownership. Gaining consensus on data definitions, for example, can be surprisingly difficult and may even cause emotional conflicts.

Data Governance Design

Governance design involves more than upper management support. Owners of the processes that generate the data and records under review by the governance body must be engaged as well as the IT staff that support the involved systems and the systems into which data or records are transmitted.

The Data Governance Institute, a consulting and training firm, describes data governance as a "system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what actions with what information, and when, under what circumstances, using what methods."[1] This boils down to deciding who will make data governance decisions and what kinds of data issues will be referred to them.

In the design phase, initially identified business data owners and data custodians from IT will serve as a model core team. These core members determine:

- Decision-making principles and protocols
- Organizational obstacles to governing data
- Mechanisms for performing data governance such as committees and processes (e.g., a budget cycle)
- Balanced stakeholder needs (e.g., HIM, compliance, insurance, clinical centers, and finance)
- Communication plans

Decision-Making Principles

The issues that drive a data governance effort usually include data integrity, standardization, uniform change management, and auditability. Decision-making protocols focus on:

- Establishing how systems will integrate and maintain data integrity, including standardization of data elements by all parties involved in the integrated systems. This is particularly important in clinical systems.
- Creating data definitions that have a common meaning across the systems employing them and a common meaning in the reporting from each system. This also applies to the standardization of definitions of metadata that will facilitate the retrieval of records from diverse systems when the organization faces litigation.
- Aligning the policies of the integrating systems (i.e., how each system has managed issues of data integrity previously and how these management practices can be standardized). New policies must define the "source of truth" for documents and records and establish the "original" that will be produced upon demand.
- Creating and documenting agreed-upon levels of data quality.
- Determining who can make what decisions about data, how records can be changed or amended, and when they may be deleted and by whom.
- Establishing required levels of documentation to support the view that the organization has "good faith" data management practices in place. This is critical to prove good faith practices under the new Federal Rules of Civil Procedure.
- Recommending ways to reduce data redundancy through standardization and consolidation of data elements and the management and development of metadata repositories.
- Making recommendations for policies and procedures that data owners, stewards, and custodians must draft and follow for long-term data and record management success.
- Determining methods and metrics to measure if data remain within the quality parameters elected by the data governance body and if documentation follows standardized record principles that allow for retrieval according to defined field parameters.
- Determining accountability and enforcement measures for nonadherence to agreed-upon data and record management quality standards.
- Creating reporting templates and mechanisms to upper management from the data governance body.

Maintaining the Gains

Good governance can speed projects forward and can create data alignments among projects, ensuring an organization's strategic objectives are achieved quickly and that work is done only once. However, there are mistakes that can defeat a data

governance effort.

Problems arise when organizations see data governance as a strictly technical function to be solved with software and consulting dollars. In reality, business unit directors and managers (likely data owners and stewards) must be engaged throughout the process. Another problem occurs when IT is detached from the objectives of the organization, which can translate into a failure to align data governance with the strategic direction of the organization.

It takes ongoing involvement and dedication of senior leaders to keep data governance consistent and on track. Painful as it may be, these committees, once formed, need to remain in place to monitor data and record quality and to enforce accountability for failure to maintain agreed-upon standards.

Members must be able to withstand political pressure to just continue doing things the way they've always been done. As information management consultant William McKnight noted, no committee can foresee the future perfectly. He suggests that organizations must proceed forward and make the best decisions they can, even if some turn out to be incorrect.[2]

Notes

1. Data Governance Institute. "The DGI Data Governance Framework." Available online at www.datagovernance.com/dgi_framework.pdf.
2. McKnight, William. "Five Top Mistakes in Information Management Governance." *Information Management Magazine*, August 2008: 48. Available online at www.information-management.com/issues/2007_50/10001722-1.html.

Sandra Nunn (snunn@phs.org) is enterprise records manager at Presbyterian Healthcare Services in Albuquerque, NM.

Article citation:
Nunn, Sandra L.. "Driving Compliance through Data Governance" *Journal of AHIMA* 80, no.3 (March 2009): 50-51.