Healthcare Data Governance

Published January 2022

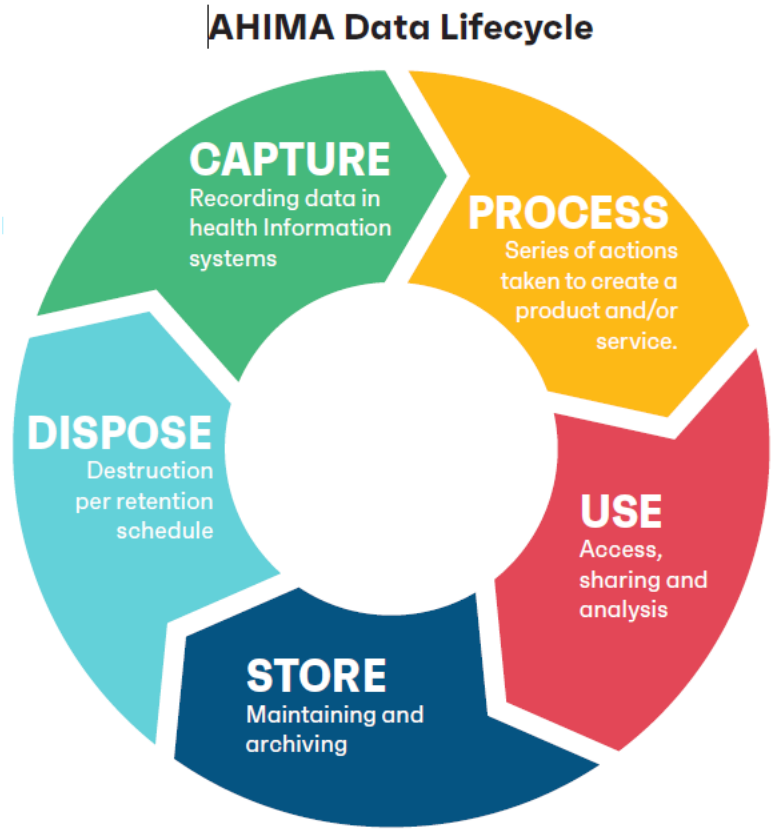
Healthcare Data Governance (DG) is not a new topic but is still challenging for many healthcare organizations to implement and achieve. With the increase in technology and specifically the electronic health record (EHR), the amount of data available has grown exponentially. Additionally, the focus on providing higher quality care in a more efficient way has increased awareness that data is a strategic asset that needs to be managed. An organization's data can consist of master data (e.g., shared data), reference data (e.g., classifications, standards, mappings), and metadata (e.g., data about other data).
This Practice Brief outlines the healthcare data governance structure/framework, guiding principles, organization-wide applications, and best practices/recommendations surrounding healthcare data.

AHIMA's Definition of Data Governance:

> The overall administration, through clearly defined procedures and plans, that assures the availability, integrity, security, and usability of the structured and unstructured data available to an organization. (AHIMA, 2020)

Healthcare data governance programs include the people, processes, and systems used to manage data throughout the data lifecycle as noted in Figure 1, allowing data to benefit the organization.

Figure 1 –AHIMA Data Lifecycle



The quality of healthcare data is vital. Ensuring data quality is often a goal of an organization's healthcare data governance program. Data quality is determined based on a set of data characteristics as summarized below.

Data Quality Characteristics

AHIMA defines Data Quality and Integrity as "the extent to which healthcare data are complete, accurate, consistent and timely throughout its lifecycle including collection, application (including aggregation), warehousing and analysis.

AHIMA characteristics of data quality are as follows:

1. Accuracy: The data should be free of errors, is correct.
2. Accessibility: Proper safeguards established to ensure data is available when needed.
3. Comprehensiveness: The data contains all required elements
4. Consistency: The data is reliable and the same across the entire patient encounter.
5. Currency: Data is current and up to date
6. Definition: All data elements are clearly defined.
7. Granularity: The data is at the appropriate level of detail.
8. Precision: The data is precise and collected in their exact form.
9. Relevancy: Data is relevant to the purpose it was collected
10. Timeliness: Documentation is entered promptly, is up-to-date and available within specified and required time frames (AHIMA 2020)

Many healthcare organizations have given some thought to data governance but perhaps are unsure where to start or how to achieve a robust data governance program. An obstacle to implementing organizational healthcare data governance may be a lack of understanding of data as an asset by key stakeholders which may lead to data silos and delays in the formation of an organizational wide program.

Healthcare data governance should be organization-wide and include interdisciplinary teams consisting of subject matter experts. A key purpose of healthcare data governance is to establish an organizational culture that ensures data is secure, reliable, and available to those who should have access to it. If the entire organization is engaged, a data governance culture is formed, leading to the organization's robust program.
A healthcare data governance culture may be achieved by starting data governance in small steps to demonstrate the value.

The first step in any healthcare data governance plan or program is to define data governance and scope. Organizations must establish the basic framework of collection, retention, use, accessibility and sharing of healthcare data. This framework may consist of policies, procedures, standards, ownership, decision rights, roles and responsibilities and accountability related to the data. Organizations should create a Data Governance Management Team (or similarly titled team) with the Chief Data Officer (or similar position

and title) working with the Chief Medical Information Officer to establish healthcare data governance plans or programs.

Governance Structure

Organizations need to establish an operational framework to determine the major DG components and their relationship to each other. High-level DG components may include structure, oversight, responsibilities, culture, regulation compliance, and infrastructure.

Charter

The purpose of the charter is to establish the Data Governance program and scope. It describes at a high level what the program will have oversight for and describes the operational framework and decision-making accountabilities required to enforce and socialize new healthcare data policies and standards.

Scope

The scope defines what the Data Governance program will include such as:

- Organizational structure
- Authorities
- Councils and roles

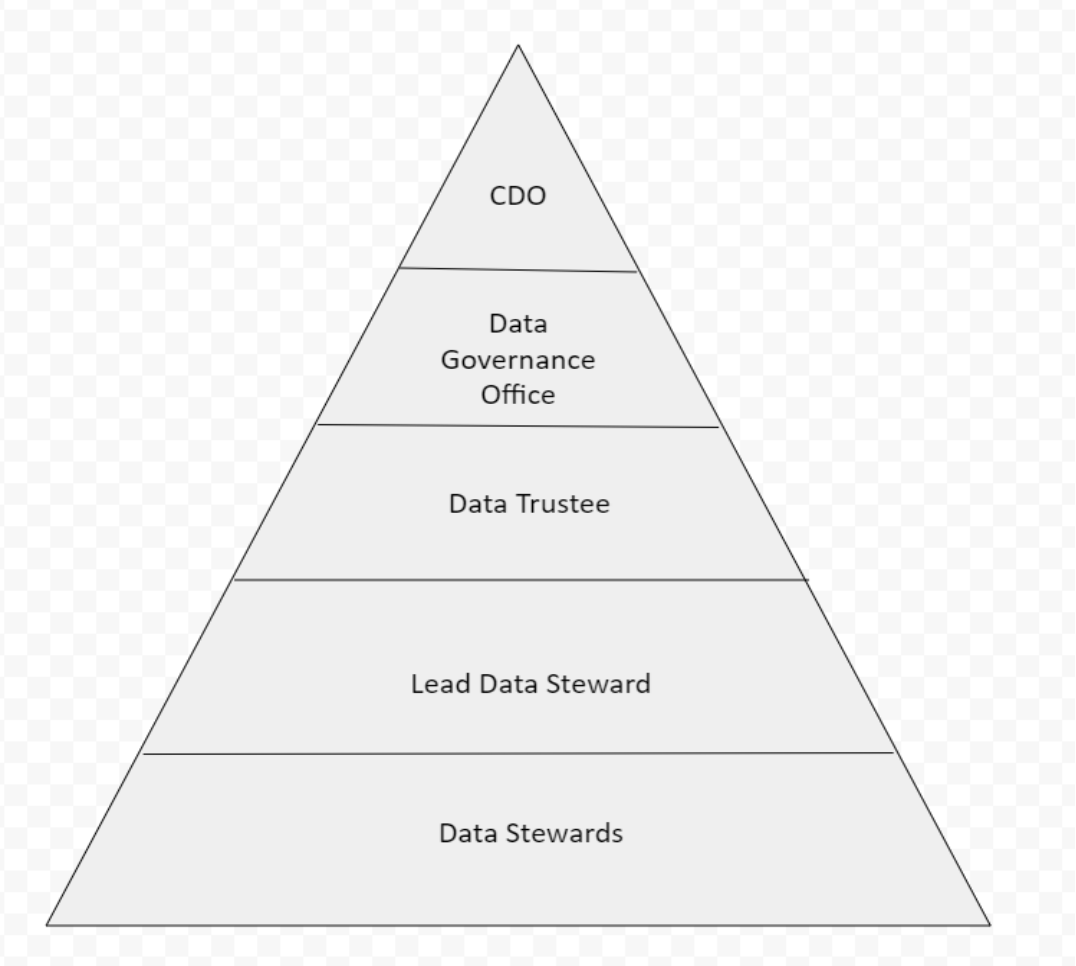
Program Guiding Principles

Examples of healthcare Data Governance program guiding principles include the following:

- Data is a strategic asset that has value and risk.
- Data related decisions should be made at the lowest level possible.
- Not all data will be treated equally; data will be valued and governed/managed based on business impact, stakeholder needs and applicable policy/regulation (e.g., protected health Information (PHI)).
- Data definitions, standards, processes, and policies will be developed and maintained with an organization-wide approach.

- Data stewards define the business terms and definitions, approve data values, data relationships, business rules, data quality standards and monitor data quality and data asset value, while IT maintains the systems that capture and manage data through their lifecycle.
- Individuals who create or acquire data are accountable for the quality of that data and must record it in accordance with its definition.
- Data quality and integrity will be addressed by the individuals that create the data and who are closest to the data, understand its meaning and business implications to the specification of the data stewards, with support from the central Data Governance program.

Figure 2 Hierarchy of Data Governance roles



KEY ROLES WITHIN THE OPERATIONAL FRAMEWORK

- Chief Data Officer (CDO)
- Chief Analytics Officer or other sponsor of the Data Governance Office or Steering Committee.
- Data Trustee
- Lead Data Steward
- Data Stewards

DATA STEWARD ROLE AND RESPONSIBILITIES

Data Steward: The Data Steward has overall accountability for data and reporting by responsibly managing data assets, data lineage, and data access, supporting sound data analysis and rationalizing information strategy. This role requires focus on data strategy, execution, and support for projects, programs, application enhancements, and production. The Data Steward defines standards and best practices for data analysis, modeling, and queries; and works collaboratively with business owners in assisting them in the accurate, timely, and complete documentation and data collection. (AHIMA, 2017) Some specific examples of responsibilities are below.

- Coordinate with organizational units and business systems to review and give input within their data domain or subdomain to the following (all which are applicable):
- Data quality and accuracy
- Data profiling
- Data queries
- Data mapping
- Business terms and synonyms
- Business definitions
- Business rules
- Conceptual data models
- List of allowable values
- Process changes
- Data standards

- Review data quality reports to ensure data is fit for the different business purposes across source systems and critical data assets.
- Act as advocates for the data and serve as the central voice representing their various stakeholder perspectives.
- Work with the Lead Data Steward in maintaining the Business Glossary in the Data Governance Platform.
- Map business terms from local systems captured within the data catalog.
- Support the dissemination and understanding of data in a data domain or subdomain both within specific jurisdiction and across the enterprise.
- Maintain an end-to-end knowledge of data and related business processes for a data domain or subdomain.
- Assign data classification, identify and document sensitive and confidential data for data elements within their data domain or subdomain.
- Provide input on data classification of data assets that contain elements from their data domain or subdomain.
- Evaluate and consult on the processes for making changes to the data model, business definitions, master data and reference data.
- Identify the value of data by liaising with stakeholders for critical business decisions
- Define data quality dimensions (timeliness, accuracy, consistency, conformity) in the source systems based on data usage.

Lead Data Stewards Role and Responsibilities

The Lead Data Stewards are data domain or subdomain specific and have deep knowledge of how data is used within the organization from a business perspective. Specifics related to this role:

- Formally appointed by the Data Trustees or the Chief Data Science Officer (owner of Analytic Data Assets).
- The appointment is reviewed annually.
- Act as an agent of the Data Trustee or the Analytic Data Asset Owner.
- Lead and coordinate efforts for associated Data Stewards within the data domain, subdomain or for an analytic data asset.
- Represent the collective of associated Data Stewards for their data domain or subdomain.

- Escalate issues to Data Stewardship Council, as appropriate, for resolution.
- Ensure policy and standards are followed, with a focus on improvement of data quality and the protection of sensitive data.
- Evaluate existing processes, controls, data flows, documentation, procedures, data lineage, and governing routines to identify gaps and/or data issues for remediation.
- Maintain all necessary artifacts needed to manage their data domain, subdomain, or analytic data asset.

Data Analytics Role and Responsibilities

The Data Analytics role oversees the creation and lifecycle management of analytic data assets. Some specific examples include the following:

- Manage and measure value creation attributed to analytic data assets.
- Ensure data use adheres to facility ethical standards and regulatory requirements (e.g., HIPAA, etc.).
- Grant access and authorization to analytic data assets.
- Adhere to definitions of data elements as defined by the Data Trustees/Lead Data Stewards for all data sourced to create analytic data assets.
- Define and manage business terms, definitions, value sets for all derived data elements and maintain them in the Business Glossary.
- Define and manage the technical metadata for all derived data elements and maintain it in the enterprise Data Catalog.
- Resolve any discrepancies with Data Trustees/Lead Data Stewards when derived data definitions are misaligned with source data elements.
- Provide training and guidance on interpretation and use of analytic data assets or visualizations/reports created from these assets.

The Data Trustees Role and Responsibilities

The Data Trustees (Owners) are senior leaders with deep knowledge and authority of the data domain or subdomain and are accountable for how data is defined and used within the facility from a business perspective. Specifics related to this role:

- Formally appointed by the Data Governance Steering Committee.
- The appointment is reviewed annually.

- Resolve conflicts escalated to the Data Trustee.
- Provide support, champion resources, and provide authority to act.
- Ensure adoption of Data Governance decisions at a national, ministry, and subsidiary levels.
- Author or contribute to key Data Governance policies.
- Identify and standardize the use and governance of data in support of the business strategy and compliance requirements.
- Approve business terms in the business glossaries and other data definitions.
- Ensure the accuracy of data as used across the organization.
- Work with other Data Trustees to resolve data issues and dissonance across business units.
- Provide input to the Steering Committee on software solutions, policies or regulatory requirements that impact their data domain.

Chief Data Officer Role and Responsibilities

The Chief Data Officer (CDO) provides vision and strategy for all data management activities, including healthcare data system lifecycles. The CDO takes the lead in global data management, governance, quality, and vendor relationships across the enterprise. Key responsibilities may include:

- Establish data policies and standards
- Lead data organization
- Master business intelligence
- Enforce organization information management concepts (AHIMA, 2017)

Policies and Procedures/ Standard Operating Procedures

Organizations may have one overall Data Governance policy or separate policies for each key area of Data Governance. Examples of key areas to address:

Data Integrity Policy: The purpose of a healthcare data integrity policy is to ensure that organizational data have integrity so that management and employees may rely on that data for decision making purposes. Data integrity refers to the reliability, accuracy, and

validity of data which requires consistent definitions for each data element and an understanding of the business processes underlying the data.

Data Access Policy: The purpose of a data access policy is to ensure that employees have appropriate access to organizational data. The value of data is increased through appropriate access. Security measures will protect data and ensure proper use of data when accessed.

Data Privacy and Usage Policy: The purpose of a data usage policy is to ensure that data are used as appropriate and according to any applicable laws. Employees may only access and use data as required for their job.

Data Sharing Policy: The purpose of a data sharing policy is to detail how internal and external data requests are inventoried, tracked, and managed and ensures data is being shared securely and efficiently. Examples would include registry data, Health Information Exchange (HIE), and research data.

Data Retention Policy: The purpose of a data retention policy is to specify how long data must be retained to meet regulatory and/or organizational needs, and what should be done to the data after retention requirements have been met. Organizations may choose to delete/destroy or archive data once retention requirements have been met.

Data Dictionary

Generally, the data dictionary is a descriptive list of the names, definitions, and attributes of data elements to be collected in an information system or database whose purpose is to standardize definitions and ensure consistent use. It supports consistent use of data, documents the source and update frequency. The data dictionary content may differ according to each organization. Basic elements are names and definitions, specific details of the data such as type, length, primary and foreign keys, and the source. The data dictionary ensures standardization and quality of the data.

Data Dictionary Example:

Field Name	Table	Description	Data Type	Field Length	Key	Valid Values	Data Source	Data Created	Field Term Date	Update Frequency
Charge Master Item	CDM	Supply Code	Text	25	Primary	Alphanumeric	Finance Office	1/1/1999		Annual
Rev Code	CDM	Rev Area	Text	4	Foreign	Digits	Finance Office	1/1/2000		Annual
HCPCS Code	CDM	HCPCS/CPT	Text	5	Foreign	Alphanumeric	Coding/HIM	1/1/2000		Annual
Charge	CDM	Charge per unit	Currency	12		>$0.00	Finance Office	1/1/2000		Annual

Business Glossary

A business glossary is a compendium of business terms and definitions, which have been approved by stakeholders and are maintained and governed. The language representing the data should be aligned with the language of the business.

Consistent terms and definitions, with corresponding metadata, are essential to managing patient demographic data across its lifecycle in the context of meaning. Agreement about term names and definitions is essential to ensure that all stakeholders who supply or consume the data understand it the same way without ambiguity. If common understanding of terms for shared data is lacking, business processes are negatively affected.

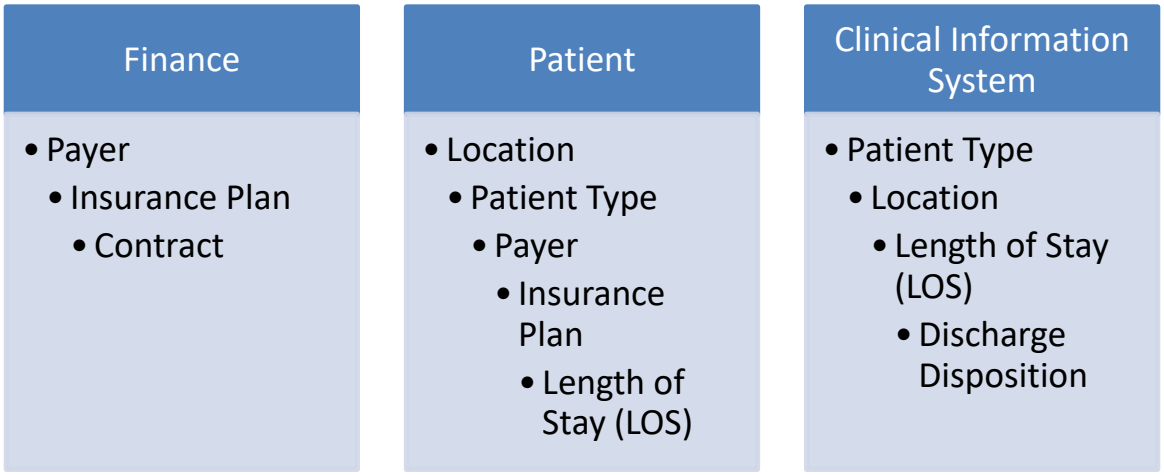
The business glossary represents agreement among key stakeholders on the language and associated meaning pertaining to patient data needed to support quality care, efficient payments, and patient safety. If business terminology is not uniquely named and defined, confusion and inefficiencies may cause issues. (The Office of the National Coordinator for Health Information Technology, n.d.)

Definitions of terms within a healthcare organization may differ by department or division. If these terms are addressed in the Business Glossary with the naming conventions and itemized by department, this will help alleviate disparities. For example: LOC may be used in

the clinical record as loss of consciousness. LOC in the surgical department may be used to identify the length of case as noted in the table below.

Application/Department/Domain	Abbreviation	Definition
Clinical Information System	LOC	Loss of Consciousness
Surgical Information System	LOC	Length of Case

All data elements within the domains of an enterprise should be included in the business glossary. Elements may overlap domains for example:



Best Practices/Recommendations

Following are some best practices and lessons learned from organizations that have implemented Healthcare Data Governance.

- Establish program priorities. Establishing program priorities helps focus Data Governance efforts to achieve results. One way to do this is to prioritize critical data elements for the organization. For example, patient demographics such as date of birth or race/ethnicity may be important as they are used in numerous ways. Key measures such as case mix or length of stay can be important to address as they are often used by multiple departments for reporting. It is important to consider where these critical data elements are used and how defined as well as the entire data lifecycle (e.g., data creation, collection, use, and destruction).
- Ensure accountability. It is important to have a Data Governance structure that helps to drive accountability. The best way to do this is to have clearly defined roles and responsibilities (e.g., sponsors, data stewards, domain owners, technical leads, etc.) -- outlining who is responsible for what and when. Having a governance structure in place allows the organization to address questions or issues as they arise as well as work toward the required goals.
- Demonstrate the value by defining key metrics. Results of the Data Governance work need to be measured and clearly demonstrate a value proposition. There should be key metrics tied to program goals. For example, key metrics may be tied to data quality (e.g., data accuracy, data completeness), risk or cost reduction (e.g., reduction in rework), or process improvement (e.g., data issues corrected). There can also be value in tracking data literacy across the organization (e.g., knowledge of data management principles; adherence to data management standards, policies, and procedures; published data definitions; attendance at trainings, etc.).

- Support collaboration. Those in Data Governance roles should have opportunities to collaborate, discuss challenges, and share best practices. Utilizing a Data Governance platform and applications can help support this effort.

Remember, establishing healthcare Data Governance is an iterative, learning process. The program will adapt and evolve over time as progress is made.

Prepared By:

Patty Buttner, MBA/HCM, RHIA, CDIP, CHDA, CPHI, CCS
Melanie Meyer, PhD, RHIA, CCS, MHA, CPHQ
Raymound Mikaelian, MSHI, RHIA
Nicole Miller, MS, RHIA
Becky Ruhnau-Gee, RHIA, CHDA, CCS, MA

Acknowledgements:
Gina Sanvik, MS, RHIA, CCS, CCS-P

Resources

AHIMA. (2020). *Health Information Management, Concepts, Principles and Practice, 6th ed.* (p. 1023), Chicago: AHIMA Press.
AHIMA. (2017) Information Governance (IG) Toolkit 3.0 (Retired)
AHIMA. (2021) *Social Determinants of Health: Improving Capture and Use by Applying Data Governance Strategies.*
The Office of the National Coordinator for Health Information Technology **https://www.healthit.gov/playbook/pddq-framework/data-governance/governance-management/**