DATA GOVERNANCE IN HEALTH CARE

Ensuring Quality and Security in Healthcare Data

DICB-UTTU Data Governance group led by Chitra Nayak, Tuskegee University

TUSKEGEE UNIVERSITY

AIM AHEAD

DATA GOVERNANCE REFERS TO THE COLLECTION OF PRACTICES, PROCESSES, POLICIES, STANDARDS, AND METRICS THAT ENSURE THE EFFECTIVE AND EFFICIENT USE OF INFORMATION IN ENABLING AN ORGANIZATION TO ACHIEVE ITS GOALS.

KEY ELEMENTS OF DATA GOVERNANCE

Data Quality Management: Ensuring the accuracy, completeness, consistency, and reliability of the data throughout its lifecycle.

Data Security and Privacy: Protecting sensitive data from unauthorized access and ensuring compliance with relevant laws and regulations, such as HIPAA for healthcare data.

Data Lifecycle Management: The handling of data from its creation and initial storage to the time it becomes obsolete and is deleted.

Data Policies and Standards: Establishing rules and guidelines for data management, including how data is collected, stored, accessed, and shared.

KEY ELEMENTS OF DATA GOVERNANCE

Data Stewardship: Assigning responsibility for data quality and lifecycle management to specific individuals or teams within the organization.

Data Compliance: Ensuring that data management practices adhere to relevant laws, regulations, and industry standards.

Data Integration and Interoperability: The ability to combine data from different sources and provide a unified view, ensuring that data across systems is compatible and usable.

DATA QUALITY MANAGEMENT

Definition: Ensures the accuracy, consistency, completeness, and reliability of data.

In Healthcare:

- **Accuracy:** Vital for correct diagnosis and treatment plans. Inaccurate data can lead to misdiagnosis or inappropriate treatment.
- **Consistency:** Consistent data formats across different systems facilitate smoother data exchange and interpretation.
- **Completeness:** Complete patient records are essential for comprehensive care, including historical health information.
- **Reliability:** Reliable data supports confident decision-making in clinical and operational aspects.

DATA SECURITY AND PRIVACY

- **Definition:** Involves protecting data from unauthorized access, breaches, and other security incidents, and ensuring compliance with privacy laws.
- **In Healthcare:**
  - **Protection of Sensitive Information:** Patient health information is highly sensitive, requiring stringent security measures.
  - **Regulatory Compliance:** Adherence to laws such as (Heath Insurance Portability and Affordability Act) HIPAA in the U.S., which sets standards for the protection of sensitive patient data.
  - **Trust:** Maintaining high standards of data security and privacy is crucial for patient trust.

DATA ACCESS AND USAGE

- **Definition:** Governs who has access to data and how data is used within an organization.
- **In Healthcare:**
  - **Controlled Access:** Ensuring that only authorized personnel have access to specific types of data, especially sensitive patient information.
  - **Usage Policies:** Establishing clear guidelines on how data can be used, including for research purposes, while respecting patient consent and privacy.
  - **Audit Trails:** Maintaining records of who accessed what data and when, which is important for security and compliance.

DATA INTEGRATION AND INTEROPERABILITY

- **Definition:** Involves combining data from different sources and ensuring that systems and software can exchange and interpret shared data.
- **In Healthcare:**
  - **System Integration:** Integrating various healthcare systems (like EMRs, billing, and patient portals) for a unified view of patient data.
  - **Interoperability Standards:** Adhering to standards such as HL7 or FHIR to ensure different healthcare systems can communicate and understand each other’s data.
  - **Facilitating Continuity of Care:** Seamless data integration allows for better continuity of care across different healthcare providers.

DEALING WITH LARGE VOLUMES OF DATA

- **Challenge:** Healthcare organizations generate vast amounts of data daily, including patient records, clinical trial data, imaging data, and more.
- **Implications:**
  - **Storage:** Managing the physical and digital storage solutions to accommodate this growing data.
  - **Processing:** Ability to efficiently process and analyze large datasets to derive meaningful insights.
  - **Accessibility:** Ensuring that relevant data is easily accessible to healthcare professionals/researchers when needed, without overwhelming them.

ENSURING DATA PRIVACY AND SECURITY

- **Challenge:** Protecting sensitive patient data from unauthorized access, breaches, and cyber threats.
- **Implications:**
  - **Compliance:** Adhering to strict regulations like HIPAA, which sets standards for the protection of sensitive patient data.
  - **Cybersecurity Measures:** Implementing robust cybersecurity protocols to safeguard data against threats.
  - **Education and Training:** Regularly training staff on the importance of data privacy and security, and how to handle data responsibly.

INTEGRATING DIVERSE DATA SOURCES

- **Challenge:** Healthcare data comes from various sources, such as electronic health records (EHRs), lab systems, imaging systems, and wearable health devices.
- **Implications:**
  - **Interoperability:** Ensuring different systems and software can effectively exchange and interpret shared data.
  - **Standardization:** Harmonizing data formats and standards across different sources for consistency and accuracy.
  - **Data Quality:** Ensuring that integrated data maintains a high quality and is usable for clinical decision-making.

ADAPTING TO CHANGING REGULATIONS

- **Challenge:** Healthcare regulations and standards are continually evolving, requiring organizations to stay current and adapt accordingly.
- **Implications:**
  - **Regulatory Tracking:** Keeping track of changes in laws and regulations that impact data governance.
  - **Agility:** Ability to quickly implement changes in processes and systems to remain compliant.
  - **Risk Management:** Proactively managing the risks associated with non-compliance, including potential legal and financial repercussions.

Structure: A data governance framework provides a structured approach to managing data across an organization. It typically includes defining the strategic objectives for data, establishing data governance roles, formulating policies and procedures, and selecting appropriate tools and technologies.

Goals: The primary goals are to ensure data accuracy, accessibility, consistency, and security, while also meeting regulatory requirements and supporting organizational objectives.

OVERVIEW OF A TYPICAL DATA GOVERNANCE FRAMEWORK

ROLES AND RESPONSIBILITIES

- **Data Governance Board or Committee:** A high-level group typically responsible for overseeing the data governance program, setting policies, and resolving major issues.
- **Data Stewards:** Individuals responsible for managing data in their respective areas, ensuring data quality, and compliance with governance policies.
- **Data Custodians:** IT staff responsible for the technical environment and data storage, ensuring data is securely stored and accessible.
- **End Users:** Healthcare professionals who utilize the data in their daily operations, responsible for adhering to data governance policies in their data handling.

POLICIES AND PROCEDURES

- **Data Quality Policies:** Guidelines to ensure data is accurate, complete, and reliable.
- **Data Security Policies:** Rules and protocols for protecting sensitive data, including patient information, against unauthorized access and breaches.
- **Data Access Policies:** Define who can access different types of data, under what circumstances, and the processes for obtaining access.
- **Compliance Procedures:** Processes to ensure adherence to regulations like HIPAA, including audit trails and reporting mechanisms.

TOOLS AND TECHNOLOGIES USED

- **Data Management Software:** Tools for data storage, processing, and analysis, such as database management systems and data warehousing solutions.
- **Data Security Tools:** Technologies like encryption, firewalls, and intrusion detection systems to secure data.
- **Data Quality Tools:** Software for data cleansing, validation, and monitoring to maintain high data quality standards.
- **Reporting and Analytics Tools:** Enable the analysis of data for decision-making and provide insights into data governance performance.
- .

Investing in Training and Awareness.

Regular Audits and Compliance Checks : Random checks, plans for non-compliance, external auditors

CALL TO ACTION FOR IMPLEMENTING DATA GOVERNANCE

Assess Current State

Develop a Strategic Plan

Invest in Training and Culture

Implement Technology Solutions

Regular Monitoring and Auditing

Engage Stakeholders

Stay Informed and Agile