Lab 06: Data Governance

1. Introduction

An organization depends on data governance as its fundamental system for controlling data assets. The framework secures data accuracy alongside accessibility and consistency and security. The report discusses data governance policy significance along with development procedures and supplies a personalized policy for the chosen organization.

---

2. What is a Data Governance Policy and Why Do We Need It?

A **data governance policy** is a formal document which establishes the management strategies for organizations to handle their data assets. The policy sets roles while defining responsibilities together with processes and standards to enable proper and accountable data utilization.

Why do we need it?

- Ensures data accuracy, consistency, and reliability.
- Complies with legal and regulatory requirements (e.g., GDPR, HIPAA).
- Improves decision-making by providing trustworthy data.
- Enhances data security and reduces risks of breaches.
- Facilitates collaboration by standardizing data practices.

---

3. Process of Developing a Data Governance Policy

The development of a data governance policy involves the following steps:

1. **Define Objectives:** Identify the goals of the policy (e.g., compliance, data quality).
2. **Identify Stakeholders:** Determine who will be involved (e.g., data owners, IT teams, executives).
3. **Assess Current State:** Evaluate existing data practices and identify gaps.

4. **Develop Policies and Standards:** Create rules for data management, access, and security.
5. **Implement Tools and Processes:** Use technology and workflows to enforce the policy.
6. **Monitor and Improve:** Continuously review and update the policy to adapt to changing needs.
7. **Exploration of Existing Templates**: Several data governance policy templates are available. Below are some observations:

What I Like:

- Clear structure which divides information with sections for goals, roles, and processes.
- Emphasis on compliance and security.
- Inclusion of data quality metrics and accountability measures.

What I Dislike:

- Various templates do not contain specialized elements that match industry requirements.
- The chosen templates include language which is difficult to non-technical stakeholders who need clarification.
- Limited focus on data inventory and content management.

---

5. Template Selection and Justification

I will use a **hybrid approach**, combining elements from templates provided by the **Data Governance Institute** and **ISO 8000**.

Reasons for Selection:

- The Data Governance Institute template provides a comprehensive structure.

- ISO 8000 emphasizes data quality, which is critical for my chosen business (healthcare).
- Both templates are adaptable to specific industries.

---

6. Data Governance Policy for Ada (Health care provider)

Business Context

I have chosen a **healthcare provider** as the business for this policy. Healthcare organizations handle sensitive patient data, making data governance essential for compliance, patient safety, and operational efficiency.

Policy Components

1. **Goals**
    - Ensure compliance with HIPAA and GDPR regulations.
    - Improve data accuracy for better patient outcomes.
    - Organizations need to implement stronger security measures which will protect patient privacy.
    - Streamline data access for authorized personnel.
2. **People**
    - **Data Governance Council:** Oversee policy implementation and compliance.
    - **Data Stewards:** Organizations need to implement stronger security measures which will protect patient privacy.

- **IT Team:** The IT Team maintains security measures for the data system while implementing its protocols.
- **End Users:** Adhere to data access and usage guidelines.

3. **Data Inventory**
    - Maintain a centralized inventory of all data assets, including:
        - Electronic Health Records (EHRs).
        - Billing and insurance data.
        - Research and clinical trial data.

    The organization should develop systems to determine data sensitivity levels which include public and confidential and restricted information.

4. **Data Content Management**
    - The organization needs standardized data formats using ICD-10 codes as an example.
    - The organization should utilize metadata management which tracks how data changes through its system.
    - The information system should perform periodic records maintenance through updated data archiving.

5. **Data Quality**
    - Define data quality metrics (e.g., accuracy, completeness, timeliness).
    - Conduct regular audits to identify and resolve data issues.
    - Establish a feedback loop for continuous improvement.

6. **Data Access**
    - The organization needs role-based access control (RBAC) to define proper data authorization protocols.
    - Require multi-factor authentication (MFA) for sensitive data.

- Selective data access activities receive logging and monitoring functions for the purpose of audits.

7. **Data Security**
    - Methods to protect data should include encryption for systems where the data remains stationary as well as while data is being transmitted.
    - The organization should train its staff through regular security sessions.
    - Perform vulnerability assessments and penetration testing.
    - Develop an incident response plan for data breaches.

---

7. Conclusion

Healthcare providers need an established data governance policy to handle data operations securely. The healthcare provider benefits from this policy by fulfilling regulatory standards while maintaining privacy safeguards and enhancing day-to-day operational performance. Organizations must use structured procedures and existing templates to develop specific data governance systems that match their operational requirements.