Care Medical - Data Governance Framework

رعاية الطبية
CARE MEDICAL

Introduction:

Data Governance Framework is a set of rules, policies, and procedures that ensure the availability, usability, integrity, and security of data used in an organization. It is a comprehensive approach to managing data assets and ensuring that they are aligned with the organization's goals and objectives. The framework provides a structure for managing data throughout its lifecycle, from creation to disposal, and ensures that data is managed in a consistent and standardized manner.

Purpose:

The purpose of a data governance framework is to establish a set of guidelines and best practices for managing data assets. It provides a framework for defining roles and responsibilities, establishing policies and procedures, and ensuring compliance with regulatory requirements. The framework also provides a mechanism for measuring the effectiveness of data management practices and identifying areas for improvement.

We follow the Data Governance framework recommended by National Data Management Office(NDMO) of Kingdom of Saudi Arabia.
The suggested frame is divided in serval Controls and Specifications under that particular control.

Control Name	**Strategy and Plan**	**Control ID**	**DG.1**
Control Description	As part of the Strategy and Plan control, the Entity shall establish a Data Management and Personal Data Protection Strategy and develop a Data Management and Personal Data Protection Plan		

The following are the Specifications under the Control Strategy and Plan:

Specification	**Data Management and Personal Data Protection Strategy**	**Specification ID**	**DG.1.1**

Introduction: Developing a robust data management and personal data protection strategy is crucial for healthcare organizations to ensure the privacy and security of patient information and other business data.

No strategy is completed without proper Vision, Mission strategic goals and objectives with approval from higher management:

Vision: Our vision is to establish a secure and trustworthy data ecosystem, where individuals' personal data is protected and managed responsibly, ensuring privacy, confidentiality, and integrity.

Mission: Our mission is to implement robust data management practices and state-of-the-art personal data protection measures to safeguard individuals' privacy rights and promote responsible data handling.

Strategic Goals:

- ***Enhance Data Governance**: Strengthen our data governance framework to ensure data is collected, processed, and stored according to strict privacy and security standards.*
- ***Foster Transparency and Trust**: Promote transparency and build trust with stakeholders by providing clear communication about how personal data is collected, used, and shared, and obtaining informed consent from individuals.*
- ***Implement Privacy by Design**: Embed privacy-centric principles and practices into our systems and processes right from the initial design phase to support data protection by default.*
- ***Enhance Security Measures**: Continuously invest in cutting-edge technologies and infrastructure to protect personal data against unauthorized access, breaches, and cyber threats.*

- ***Empower Individuals***: *Educate and empower individuals about their rights regarding personal data, enabling them to make informed choices and have control over their data.*

Objectives:

- *To develop and implement a comprehensive data protection policy and ensure its compliance across the organization.*
- *Conduct regular data audits and risk assessments to identify vulnerabilities and implement necessary security measures.*
- *Establish a robust incident response plan to promptly and effectively address data breaches, minimizing potential harm to individuals by using our established Incidence reporting system in place.*
- *Offer training programs and resources to employees to enhance their awareness and understanding of data management and protection practices including cyber threats.*

Here are some key considerations included in the strategy:

Data Governance: Establish a clear framework for managing data within the organization. This includes defining roles and responsibilities, data ownership, and data lifecycle management.

Data Classification: Classify data based on its sensitivity and criticality. This will help determine the appropriate level of security controls and access rights for different types of data.

Data Protection: Implement strong security measures to protect data from unauthorized access or breaches. This includes using access controls, firewalls, and regular security audits.

Consent Management:
Develop policies and procedures to obtain and manage patient consent for data collection, use, and disclosure. Ensure compliance with applicable laws and regulations, such as The Personal Data Protection Law (PDPL) of Saudi Arabia depending on scope of NMC and its business units.

Data Retention and Disposal:
To minimize data retention risks and ensures compliance with legal requirements Care Medical company follow the data retention policy in place and related Health Information Management and Leadership policies.

Staff Training and Awareness:
Provide regular training to employees on data protection best practices, privacy laws, and cybersecurity. This reduces the likelihood of human error or negligence leading to data breaches.

Incident Response Plan:
Developed a comprehensive incident response plan to address potential data breaches or security incidents swiftly and effectively. This includes the enterprise Incident reporting practice through our intranet 'Mycare'.

Compliance Monitoring:
Q.I department regularly monitor and audit the all types of Incidence reported.They do analysis and report to the Hospital management committees. They also has KPI's in place related to incidence reporting by type.

Specification	Data Management Guiding Principles	Specification ID	DG.1.2

NMC and its business units are committed to follow the guide principal provided by National Data Management and Personal Data Protection standards by Saudi government entities based on a defined compliance assessment methodology.

Principle	Definition	Mapped Domain(s)
Data as a National Asset	As any public sector asset, Government data should be discoverable, protected and Maintained with clear accountability and with the potential to be monetized.	• Data Governance
Data Protection by Design	Build systems and processes that are proactive in protecting the privacy of individuals as well as their right to consent and/or refuse under the applicable KSA laws.	• Personal Data Protection • Data Classification • Data Security and Protection
Open by Default	Ensure that the Government avail most of its data to the public by default unless there is sufficient justification that non-disclosure of data is of greater public interest.	• Open Data
Ethical Data Use	Build ethical practices and norms around the governance and usage of data with fairness, traceability and contribution to the "Common Good" at the heart of these practices in alignment with the tenants of the Saudi culture.	• Data Governance
Purposeful Design	Adopt a human-centric and responsive approach for data collection, processing, sharing, and usage to meet the future needs of the Kingdom.	• Data Operations • Data Sharing and Interoperability • Data Architecture • Reference and Master Data Management
Data-Driven Outcomes	Build the next Generation Public Sector where most of the operational and strategic decisions as well as policy formulation are based on data insights.	• Business Intelligence and Analytics • Data Value Realization
Learning Culture	Build trust among the Government and with the Public either through ensuring high quality data or by being transparent about the level of quality.	• Data Quality • Reference and Master Data Management • Data Catalog and Metadata • Document and Content Management

Specification	Data Management and Personal Data Protection Plan	Specification ID	DG.1.3

Data management and personal data protection are significant considerations in today's digitized world. Developing a comprehensive plan is crucial for organizations to ensure the responsible handling of data. Here are some key aspects which are included in our plan:

1. ***Data Inventory:***
   The goal of data inventory recording is to create a comprehensible and organized system that allows easy access and retrieval of information. We identify all types of data collected, processed, and stored within our organization, including personal data. Also our staff understand how their domain specific data is gathered, used, and shared.

   Following is the data inventory:
   - HR and Administrative Data
   - Physicians and Paramedics Information
   - Medical licenses and certifications
   - Financial Data
   - Marketing Data
   - Property Control data
   - Supply Chain Management Data
   - Vendor and Supplier Information
   - Patient Demographic Information
   - Appointment scheduling data
   - Patient Insurance Information
   - Insurance provider details
   - Policy related data
   - Claims related data
   - Billing and Claims reimbursement data
   - Medical history
   - Treatment records
   - Diagnostic test results
   - Medication history
   - Allergies and adverse reactions
   - Health Information management
   - Electronic Medical Records (EMR)
   - Vital signs
   - Progress notes
   - Laboratory test results
   - Radiology reports
   - Surgical reports
   - Consent and other forms
   - User access logs
   - Website Analytics Data
   - Mobile apps data

2. *Data Classification:*
Categorize your data based on its sensitivity and potential risks. Label personal data separately to prioritize its protection. The data stewards will provide the data classification related to their area or department with the classification. Based on that the enterprise data classification table will be build.

3. *Consent Management*:
Obtain appropriate consent from individuals before collecting and processing their personal data. It will ensure that the consent is freely given, specific, informed, and can be withdrawn at any time. We will stick to the Organization wise consent policy related to Patients.

4. *Data Security*:
Implement robust security measures to protect personal data from unauthorized access, loss, or alteration. This may include encryption, access controls, and regular security audits.

5. *Data Processing Agreements*:
Establishing agreements and MOU's with third parties who process Patient, Personal data of Staff in our behalf. Ensure these agreements clearly outline responsibilities, security measures, and data protection obligations.

6. *Data Breach Response*:
Develop a data breach response plan to handle security incidents promptly and effectively. This includes notifying affected individuals and authorities, assessing the impact, and taking appropriate remedial measures. Data breach incidences will be handled by Enterprise Incidence Reporting system which is already implemented in our organization.The option is present in intranet system 'Mycare'.

8. *Staff Training and Awareness*:
We provide regular training to employees on data protection best practices by conducting cyber security awareness lecture and training programs. Also encourage a culture of data privacy awareness within our organization by inducting the lectures in induction program for new employees and periodic lectures also for the compliance of accreditations like JCIA, CBAHI etc.

9. *Compliance and Auditing*: We try to stay up to date with relevant data protection regulations and standards. Conduct regular internal audits to ensure compliance with these requirements.

Specification	Strategy Approval and Socialization	Specification ID	DG.1.4

Formation of Data governance committee:

The Data governance committee is formed which has following structure:

- Chairmanship of the committee: CIO
- CO- Chairmanship of the committee: Director of Governance Risk and Compliance.
- Members of the Committee:
  Data Officer: Member from IT department
  Governance Officer: GRC department
  Risk Officer : GRC department

Approval of Higher management:

This committee is approved by the CEO.

Control Name	Policy and Guidelines	Control ID	DG.2
Control Description	As part of the Policy and Guidelines control, the Entity shall conduct a Data Management and Personal Data Protection Policy and Guidelines gap analysis, and develop the Entity specific Data Management and Personal Data Protection Policy and Guidelines.		

Specification	Gap Analysis - Data Management and Personal Data Protection	Specification ID	DG.2.1

The Gap Analysis was performed within the organization after reading the guidance from NDMO.

After the analysis, it was found that the required policy 'Data Management and Personal Data Protection' is not present.

Gap Analysis was performed and brain storming session with Data Governance team.

2. Importance of Gap Analysis in Data Management and Personal Data Protection:

- Understanding Data Management and Personal Data Protection
- What constitutes Data Management?
- What constitutes Personal Data Protection?
- Examples of Data Management and Personal Data Protection.

3. Adopted Gap Analysis Process:

- Discussion with Data Governance Task Force
- Reviewed present Policies and Procedures
- Speak to Key Stakeholders.

4. Conclusion:

Encouraging best practices for Gap Analysis in Data Management and Personal Data Protection after reading the different success stories of the organization around the globe and research on some websites advocating Data Management and Governance.

Specification	Policy - Data Management and Personal Data Protection	Specification ID	DG.2.2

Signatory Approvals:

Engr. Ibrahim Al-Ammar
Chief Information Technology Officer

Collaborating Department:

Mr. Adel Al-Jabrati
Director, Governance, Risk Management & Compliance

Approved By:

Dr. Abdulaziz Al-Obaid
Chief Executive Officer