CARE Medical Company

DATA GOVERNANCE

Operating Manual:	Data Governance			Policy No.	CMC-DG-01
				Version No.	1
Title/Description:	**Data Governance Framework**				
Initial Issue Date: 1st October 2023	**Effective Date:** 24 November 2024	**Due for Review:** October 2027	**Applies To:** CARE Medical and Business Units		**Replaces:** N/A

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) under SDAIA 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.

Operating Manual:	Data Governance		Policy No.	CMC-DG-01
			Version No.	1
Title/Description:	**Data Governance Framework**			
Initial Issue Date: 1st October 2023	**Effective Date:** 24 November 2024	**Due for Review:** October 2027	**Applies To:** CARE Medical and Business Units	**Replaces:** N/A

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:

Operating Manual:	Data Governance		Policy No.	CMC-DG-01
			Version No.	1
Title/Description:	**Data Governance Framework**			
Initial Issue Date: 1st October 2023	**Effective Date:** 24 November 2024	**Due for Review:** October 2027	**Applies To:** CARE Medical and Business Units	**Replaces:** N/A

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 have KPI's in place related to incidence reporting by type.

Specification	**Data Management Guiding Principles**	**Specification ID**	**DG.1.2**

CMC 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

Operating Manual:	Data Governance		Policy No.	CMC-DG-01
			Version No.	1
Title/Description:	**Data Governance Framework**			
Initial Issue Date: 1st October 2023	**Effective Date:** 24 November 2024	**Due for Review:** October 2027	**Applies To:** CARE Medical and Business Units	**Replaces:** N/A

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

Operating Manual:	Data Governance		Policy No.	CMC-DG-01
			Version No.	1
Title/Description:	**Data Governance Framework**			
Initial Issue Date: 1st October 2023	**Effective Date:** 24 November 2024	**Due for Review:** October 2027	**Applies To:** CARE Medical and Business Units	**Replaces:** N/A

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

Operating Manual:	Data Governance		Policy No.	CMC-DG-01
			Version No.	1
Title/Description:	**Data Governance Framework**			
Initial Issue Date: 1st October 2023	**Effective Date:** 24 November 2024	**Due for Review:** October 2027	**Applies To:** CARE Medical and Business Units	**Replaces:** N/A

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 and Employees.

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'

7. **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. Regular banners and posters are displayed on MyCare and also send by emails.

8. **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

Operating Manual:	Data Governance	Policy No.	CMC-DG-01
		Version No.	1
Title/Description:	**Data Governance Framework**		

Initial Issue Date:	Effective Date:	Due for Review:	Applies To:	Replaces:
1st October 2023	24 November 2024	October 2027	CARE Medical and Business Units	N/A

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 CEO of CARE Medical Company (CMC)

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

1. **Introduction:**
   The Gap Analysis was performed within our organization after reading the guidance from NDMO guide

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

   We performed Gap Analysis and brain storming session with our 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:**

Operating Manual:	Data Governance		Policy No.	CMC-DG-01
			Version No.	1
Title/Description:	**Data Governance Framework**			
Initial Issue Date: 1st October 2023	**Effective Date:** 24 November 2024	**Due for Review:** October 2027	**Applies To:** CARE Medical and Business Units	**Replaces:** N/A

- 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

1.0 Objective
To contribute in the vision and mission of the KSA National Data Management and Personal Data Protection Standards Specifications by establishing the Data Governance Framework and establish the guidelines.

A Data Management and Personal Data Protection Policy is crucial to ensure the proper handling and safeguarding of sensitive information and comply with applicable laws and regulations.
Ensuring the confidentiality and integrity of personal data, protecting the rights and privacy of individuals, maintaining compliance with relevant data protection laws, or establishing best practices for data management within the organization.
Hence we adopted the definitions and guidelines from the Data Protection Law published by Saudi Data and AI authority (SDAIA). Version - Amended pursuant to Royal Decree No.(M/148) DATED 05/09/1444 AH Corresponding to 27/03/2023 G.

Definitions:
1- Personal Data: Any data, regardless of its source or form, that may lead to identifying an individual specifically, or that may directly or indirectly make it possible to identify an individual, including name, personal identification number, addresses, contact numbers, license numbers, records, personal assets, bank and credit card numbers, photos and videos of an individual, and any other data of personal nature.

2- Processing: Any operation carried out on Personal Data by any means, whether manual or automated, including collecting, recording, saving, indexing, organizing, formatting, storing, modifying, updating, consolidating, retrieving, using, disclosing, transmitting, publishing, sharing, linking, blocking, erasing and destroying data.

3- Collection: The collection of Personal Data by Controller in accordance with the provisions of this Law, either from the Data Subject directly, a representative of the Data Subject, any legal guardian over the Data Subject or any other party.

4- Destruction: Any action taken on Personal Data that makes it unreadable and irretrievable, or impossible to identify the related Data Subject.

5- Disclosure: Enabling any person - other than the Controller or the Processor, as the case may be - to access, collect or use personal data by any means and for any purpose.

Operating Manual:	Data Governance		Policy No.	CMC-DG-01
			Version No.	1
Title/Description:	**Data Governance Framework**			
Initial Issue Date: 1st October 2023	**Effective Date:** 24 November 2024	**Due for Review:** October 2027	**Applies To:** CARE Medical and Business Units	**Replaces:** N/A

6- Transfer: The transfer of Personal Data from one place to another for Processing.

7- Publishing: Transmitting or making available any Personal Data using any written, audio or visual means.

8- Sensitive Data: Personal Data revealing racial or ethnic origin, or religious, intellectual or political belief, data relating to security criminal convictions and offenses, biometric or Genetic Data for the purpose of identifying the person, Health Data, and data that indicates that one or both of the individual's parents are unknown.

9- Genetic Data: Any Personal Data related to the hereditary or acquired characteristics of a natural person that uniquely identifies the physiological or health characteristics of that person, and derived from biological sample analysis of that person, such as DNA or any other testing that leads to generating Genetic Data.

10- Health Data: Any Personal Data related to an individual's health condition, whether their physical, mental or psychological conditions, or related to Health Services received by that individual.

11- Health Services: Services related to the health of an individual, including preventive, curative, rehabilitative and hospitalizing services, as well as the provision of medications.

12-Credit Data: Any Personal Data related to an individual's request for, or obtaining of, financing from a financing entity, whether for a personal or family purpose, including any data relating to that individual's ability to obtain and repay debts, and the credit history of that person.

13- Data Subject: The individual to whom the Personal Data relate.
14- Public Entity: Any ministry, department, public institution or public authority, any independent public entity in the Kingdom, or any affiliated entity therewith.
15- Controller: Any Public Entity, natural person or private legal person that specifies the purpose and manner of Processing Personal Data, whether the data is processed by that Controller or by the Processor.
16- Processor: Any Public Entity, natural person or private legal person that processes Personal Data for the benefit and on behalf of the Controller.

2.0 Purpose and Scope

Purpose:

The primary objective of this policy is to ensure the secure and responsible management of personal data within our healthcare organization. We strive to maintain the confidentiality and integrity of patient information, while also safeguarding the rights and privacy of individuals in compliance with applicable healthcare and data protection regulations. By establishing robust data management practices, we aim to enhance patient trust, protect sensitive healthcare data, and enable effective healthcare delivery and catering the data needs of external agencies requesting data.

Scope:

Operating Manual:	Data Governance		Policy No.	CMC-DG-01
			Version No.	1
Title/Description:	**Data Governance Framework**			
Initial Issue Date: 1st October 2023	**Effective Date:** 24 November 2024	**Due for Review:** October 2027	**Applies To:** CARE Medical and Business Units	**Replaces:** N/A

The scope of data management guidelines encompasses several aspects, including the types of data collected, processed, and stored by the NMC and its business units. This includes patient medical records, health information, diagnostic reports, and other relevant data. The guidelines also cover the handling of sensitive personal information, such as social security numbers, insurance details, and any other personally identifiable information (PII) related to patients.

The scope outlines the responsibilities of NMC as the healthcare organization in terms of proper data collection, storage, access controls, data sharing, and data retention periods. It ensures that personal data is handled in accordance with applicable laws, regulations, and industry best practices, such as the Personal Data Protection Law Article-4 prescribed by SDAIA.

1- The Law applies to any Processing of Personal Data related to individuals that takes place in the Kingdom by any means, including the Processing of Personal Data related to individuals residing in the Kingdom by any means from any party outside the Kingdom. This includes the data of the deceased if it would lead to them or a member of their family being identified specifically.
2- The scope of applying the Law excludes the individual's Personal Data Processing for purposes that do not go beyond personal or family use, as long as the Data Subject did not publish or disclose it to others. The Regulations shall define personal and family use provided in this Paragraph.

3.0 General Policy

This policy is in place to ensure the responsible handling of data. Therefore, this policy outlines how an organization collects, manages, and protects data, as well as how it is used and shared.

Here are some key elements to be consider for this policy:

1. Data Collection and Use: Describe how data is collected, ensuring it's done lawfully. Specifies the purpose for collecting data, how it will be used, and outline any third parties that may have access to the data.

1. Data Collection: The following types of the personal data is collected:

Data collection Particulars	Means of Data Collection
Personal information of Employees required for HR	Forms in HR Module in "Careware" System
Demographic Information for Patients	Forms in Medical System in "Careware" system
Patients medical history	Web EMR in HIS system "Careware"
Patients all Medical test results	From PACS system and LIS data is push to Web EMR in HIS system "Careware".
Services provided to the Patients like Medicines and procedures etc.	Web EMR in HIS system Careware
Patient's Insurance coverage data	Insurance module in HIS system "Careware"
Medical Reports and Medical History	Web EMR in HIS system Careware.

Operating Manual:	Data Governance		Policy No.	CMC-DG-01
			Version No.	1
Title/Description:	**Data Governance Framework**			
Initial Issue Date: 1st October 2023	**Effective Date:** 24 November 2024	**Due for Review:** October 2027	**Applies To:** CARE Medical and Business Units	**Replaces:** N/A

Personal Data collection is also supported by the following policies and should follow guidelines mentioned in this policy:

Policy Name	Custodial Department	Purpose
Management of Personnel File	HR	This policy applies to all Staff in every Administration/ Department within CARE in order to inform staff of the etiquettes that will apply to the safekeeping of their personal file. Employee details and files are kept centrally under Personnel Department within Human Resources Administration.
Confidentiality of Patient's Medical Record Information	HIM	To ensure that all data and information in patient medical records are confidential, and that all hospital personnel are aware that they have an obligation to protect the confidentiality of the patient's health information.
Protection of Medical Records	HIM	To establish a process of protecting the medical records from loss, theft, deliberate alterations or destructions by fire, water damage, pest damage, or with changes in area temperature and humidity.
Release of Medical Records	HMI	1.To establish a well-defined mechanism for the release of Medical Records to Inpatient and Outpatient clinical areas of Care Medical Centers in order to facilitate appropriate and timely patient care management in a manner that ensures security and confidentiality of patient information. 2. To further establish the limitations in which a Medical Record can be released for any reasons not related to direct patient care such as research and study, utilization management, quality and patient safety reviews (Morbidity, Mortality, Patient Complaints), governmental requests, and medico-legal investigations.

		3. To provide a copy of the patient's Medical Record upon authorized request from a Lawyer through the Malpractice Committee at the Ministry of Health. 4. To establish a process of protecting the records and information from loss, damage, destruction, tampering & unauthorized access or use.
Release of Information (Hospital Wide).	HIM	To ensure that all patient information are confidential, and that all hospital personnel are aware that they have an obligation to protect the confidentiality and policy to release of the patient's health information.

3. **Consent**: We have Patient consent policy, which emphasize the importance of obtaining patient consent for data collection, ensuring that patients are fully informed about how their data will be used and shared. It also outlines procedures for obtaining consent and inform patients of their right to withdraw consent at any time. This all is covered by the following policies:

Policy Name	Custodial Department	Purpose
Home Health Care Patient Consent, Refusal/ Withdrawal of Care.	Home Healthcare Services	To obtain a consent through a process defined by the Home Health Care (HHC) and carried out by trained staff in a manner and language that the patient can understand.
Patient Informed Consents	HIM	• Maintain and secure patient's rights. • Provide information to the patient. • Provide choices for the decision making regarding health care. Avoid litigation.
General Consent for Treatment	Patient Services Department	• To render all routine necessary for the inpatient and outpatient medical care. • Provide information about scope of care shall be given to the patient. • Provide choices for the decision making regarding health care. • Maintain and secure patient's rights

Operating Manual:	Data Governance		Policy No.	CMC-DG-01
			Version No.	1
Title/Description:	**Data Governance Framework**			
Initial Issue Date: 1st October 2023	**Effective Date:** 24 November 2024	**Due for Review:** October 2027	**Applies To:** CARE Medical and Business Units	**Replaces:** N/A

4. **Data Storage and Security:** The policy address how patient data is stored securely, whether through physical or digital means. It addresses measures taken to protect against unauthorized access, breaches, and data loss, including encryption, firewalls, and access controls. Also to maintain confidentiality of Medical records of the Patients.

   The following Policies covers the activities related to Data Storage and Security.

Policy Name	Custodial Department	Purpose
Data Security, Confidentiality and Protection.	NMC IT Department	The general purpose of the Information Technology Security Policy is to reduce the potential risks of unauthorized modification, destruction or disclosure of information whether intentional or accidental while Maintaining confidentiality, integrity and availability of NMC CARE and its business unit's data.
Data Backup	NMC IT Department	1. To safeguard the information assets of NMC and its BU. To prevent the loss of data in the case of an accidental deletion or corruption of data, 3. To permit timely restoration of information and business processes, should such events occur. 4. To manage and secure backup and restoration processes and the media employed in the process.
Disaster Recovery Plan	NMC IT Department	This document delineates company policies and procedures for technology disaster recovery, as well as process-level plans for recovering critical technology platforms and the telecommunications Infrastructure. record retention and to destroy the medical records according to decided schedule for disposal as per policy.
Confidentiality of Patient's Medical Record Health Information	Health Information Management (HIM)	To ensure that all data and information in patient medical records are confidential, and that all hospital personnel are aware that they have an obligation to protect the confidentiality of the patient's health information.

5. **Data Accuracy and Retention and Destruction:** We established guidelines for maintaining accurate and up-to-date data. Define retention periods for different types of data and outline procedures for secure disposal when data is no longer needed. This is covered by the supporting Organization wise policies:

Operating Manual:	Data Governance			Policy No.	CMC-DG-01
				Version No.	1
Title/Description:	**Data Governance Framework**				
Initial Issue Date: 1st October 2023	**Effective Date:** 24 November 2024	**Due for Review:** October 2027	**Applies To:** CARE Medical and Business Units		**Replaces:** N/A

Policy Name	Custodial Department	Purpose
Documents retention and destruction	Leadership and Hospital Management	To establish a policy and procedure applied hospital wide for the electronic or paper based documents retention period and destruction conditions and requirements.

6. **Data Subject Rights:**
Our medical centers have wall mounted posters showing the Patients wrights and also the medical staff is trained and explain the Patients about their rights regarding their personal data. Include procedures for handling requests to access, correct or restrict data processing.

Patient Services Department policy for Patient Rights and also the Health Information Management department has their policies in this regards.

Policy Name	Custodial Department	Purpose
Information Privacy, Confidentiality and Security	Leadership and Hospital Management	How to maintain Information Privacy , Confidentiality and Security
Patient and Family Rights, Responsibility	Patients Services	Patient and Family Rights in Riyadh Care Hospital (RCH) shall be based on Saudi laws, regulations, and national accreditation requirements. It shall be safeguarded by policies, procedures and practices.

7. **Data Breach Response:** We have protocols for detecting, reporting, and mitigating data breaches. Outline the steps to be taken in the event of a security incident, including notification of affected individuals and relevant authorities.

- The employees are always encouraged through lectures and initiatives by Q.I department to report such incidences.
- The incidence reporting tool is provided in our intranet 'Mycare'. The individual's identity is also kept secret.
- Complete investigation is done and preventive actions are taken in coordination of Q.I department.
- Incidence Reporting KPI's are maintained by Q.I department.

Operating Manual:	Data Governance		Policy No.	CMC-DG-01
			Version No.	1
Title/Description:	**Data Governance Framework**			
Initial Issue Date: 1st October 2023	**Effective Date:** 24 November 2024	**Due for Review:** October 2027	**Applies To:** CARE Medical and Business Units	**Replaces:** N/A

Policy Name	Custodial Department	Purpose
Information Privacy, Confidentiality and Security	**Leadership and Hospital Management**	**How to maintain Information Privacy, Confidentiality and Security**

8. **Employee Training and Accountability:** Provide regular training to ensure awareness of policies and procedures.

   Also IT department will provide the Cyber, Data and Information Security awareness trainings.

   The arrangements for the training will be done at the time of New employee's induction program also as and when required.