وزارة الصحة
Ministry of Health

Data Governance Policy

وزارة الصحة

Table of content

1. Introduction

This document defines the Data Governance policy and the sections below cover purpose, scope, and details for each data domain of data governance policy. It also covers respective roles & responsibilities aligned with MoH Data Governance Target Operating Model for each data domain.

1.1. Policy Purpose

The purpose of this policy is to establish directives for effectively managing and governing MoH data assets. This document covers policy statements for each in-scope data domain specified in the MoH Data governance charter. Following 14 data domains are covered as part of the data governance policy document:

1. Data Governance Office
2. Data Catalog and Metadata
3. Data Quality
4. Data Operations
5. Document and Content Management
6. Data Architecture and Modelling
7. Reference and Master Data Management
8. Business Intelligence and Analytics
9. Data Sharing and Interoperability
10. Data Value Realization
11. Open Data
12. Freedom of Information
13. Data Classification
14. Personal Data Protection

1.2. Policy Scope

This policy applies to all data & information handled by MoH whether stored in electronic or physical form. This policy further applies to all MoH Organization units, data domains, sub-data domains, MoH employees, or contractors, vendors, third party service providers, or their staff or agents.

1.3. Scope of work

The KSA, Ministry of Health manages a significant amount of personal and health data, crucial for healthcare services. This sensitive information includes medical history and treatments. MoH takes great responsibility for the privacy and security of this data, using it for healthcare delivery, research, and policy formulation. Strict measures, such as encryption and access controls, are in place to protect the information. Collaboration with healthcare providers ensures seamless data exchange, reflecting MoH's commitment to responsibly handle and safeguard individuals' personal and health data.

1.4. Abbreviations

MOH	Ministry of Health
CDE	Critical Data Element
DBMS	Database Management System
DG	Data Governance
DC	Data Classification
PDP	Personal Data Protection
DGH	Data Governance Head
DPIA/PIA	Data Protection Impact Assessment or Personal Data Protection Assessment or Privacy Impact Assessment
FOI	Freedom of Information
KPI	Key Performance Indicator
KSA	Kingdom of Saudi Arabia
NCA	National Cybersecurity Authority
NDMO	National Data Management Office
Entity	Open Data & Information Access Officer
ROI	Return on Investment
PDPL	Personal Data Protection Law

1.5. Definitions

Accountability Principle	Organizations shall take responsibility for processing the personal data of data subjects & shall be able to demonstrate compliance to the following six principles: -Lawfulness, Fairness &Transparency principle -Purpose Limitation principle -Data Minimization principle -Accuracy principle -Storage Limitation principle -Integrity & Confidentiality principle
Attribute Registration	Capturing the Key data attributes/ Critical Data Elements (CDE) of the data domains
Accuracy Principle	The personal data processed shall be kept accurate, complete & up-to-date wherever possible. Every reasonable step must be taken to ensure that any inaccurate personal data is erased or rectified without delay
Authoritative Data Sources	A repository or system that is the primary or most reliable source of data and is authorized to share that data with other systems.
Business Glossary	It is an inventory of all business terms with attributes for context such as business definition, business rules, policies, classification of the data which are used by the departments in the day-to-day operations.
Business Rules	Business rules are business-specific verifiable statements that are identified for each CDE.
Charging Model	The adopted method that defines how customers are charged for products or services
Consent	'Consent' of the data subject means any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action,

	signifies agreement to the processing of personal data relating to him or her Consent is considered 'explicit' if it is provided via a clear statement, e.g., ticking a checkbox for a clearly written consent statement, by means of his signature to a clearly written statement, via email, etc.
Cool-off period	Cool-off period is a defined period between data archival and data deletion given to the business before data is disposed of. This period is used to gauge if there are any operational impacts owing to non-availability of the data that is to be disposed of.
Cost Saving Use Case	Implemented use case that resulted in a data or data product that achieves cost savings for the organization
Dataset	Data arranged in a systematic or methodical way and accessible by electronic or other means
Data Acquisition	Data acquisition is the process of extracting data from internal or external sources such as acquiring data from the vendors, or getting the data from internal source systems, etc.
Data Controller	Any natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data
Data Governance	Data Governance is the exercise of authority and control (planning, monitoring, and enforcement) over the management of data assets
Data Governance Approval Register	Data Governance Approvals Register refers to the document to store the approver name, approved date, approval remarks, status provided for each data governance domain.
Data Governance Issue Tracking Register	Data Governance Issue Tracking Register refers to the document to capture the issues raised under each data governance domain. Here, information such as Issue ID, Issue Description, Issue Type, Issue Raised By, Issue Raised Date and Issue Resolution Date are captured.
Data Governance Version Control	Data governance version control refers to the document to capture the modifications made to each data governance domain policy, process and control. Here, information such as Version ID, Created By, Modified By, Modification Description and Modified Date are captured.
Data Labels	Data labels are tags that can provide some information regarding the data asset such as if it contains personal data and its classification level, retention period, archival period, deletion period, etc.
Data Lineage	Data Lineage provides a broad understanding of origination, movement and transformations applied to data over time.
Data Maintenance	Data maintenance is the process of keeping data in the proper conditions and formats as required.
Data Minimization Principle	It implies that the personal data being processed shall only be limited to the amount necessary to fulfil the processing purpose and no additional personal data shall be processed.
Data Processing (data operations)	Any operation or set of operations which is performed on data or on sets of data such as recording, structuring, profiling, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, etc.
Data Processor	An entity that processes personal data on behalf of a data controller
Data Product	A product that utilizes data to deliver a service to the end-user. For example, performing data analysis on customer data to aggregate

	information about customer segments and leverage the analytics results for various business purposes
Data Protection Principles	Principles or rules the embody the spirit of personal data protection
Data Privacy & Protection Manager	This role is responsible for overseeing personal data protection compliance within an organization & representing the organization to the public
Data Retention Preparation	Data Retention preparation is the process of making the data ready for retention in the relevant systems through processes such as data classification and labelling.
Data Subject	Any natural person to whom the personal data relates to, or his representative, or the person who has legal custody over him/her
Data Value Realization	The identification, planning, implementation of data driven use cases that with potential for revenue generation or cost reduction and solving business problems
Escalation Matrix	The Data Governance Issues shall be escalated in the ascending order in 3-tier structure. Firstly, this issue will be taken up by the Data Governance Working Group, and then it will be escalated to the Data Governance Council and then it will be escalated by the Data Governance Steering Committee.
Integrity & Confidentiality (Security) Principle	This principle implies that the personal data shall be processed in a manner that ensures appropriate security of the personal data. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
Issue management	Issue management is the process of identifying and resolving issues
Lawfulness & Transparency Principle	This principle implies that the personal data shall be processed in a lawful, fair & transparent manner. Processing is lawful if data subject consent is received, processing for legal, regulatory or contractual obligations, to protect the vital interests of the data subject, or for legitimate interests of the organization, where such interests do not pose any risk to data subjects
Metadata	Metadata is data about data. Metadata helps an organization understand its data, its systems, and its workflows. Metadata is of three types - Business metadata, Technical metadata and Operational metadata.
NDMO Data Management Standards	NDMO developed the Data Management and Personal Data Protection Standards for implementing and governing effective data management practices across government entities
Number of Data or Data Products revenue generation request	A request raised to the regulatory authority (NDMO) for approving implementation of the revenue generating data or data product
Open Data	Open data is publicly available data that can be reused, re-distributed & combined with other datasets (following open data license norms) for further analysis
Personal Data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

Personal data breach	Disclosure, acquisition, or access to personal data in unauthorized form or in absence of a legal basis, whether intentionally or unintentionally
Personal Data Processing	Any operation or set of operations which is performed on personal data or on sets of personal data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, profiling, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Profiling	Any form of automated processing of personal data consists of the use of personal data to evaluate certain personal aspects relating to a natural person, to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
Purpose Limitation Principle	This principle implies that the personal data shall be collected against specific & legitimate purposes & shall be only processed in a manner that is compatible with those purposes
Records of Processing Activities	An inventory of the various types of personal data processing operations performed in an organization
Service Level Agreement	A contract between a service provider and service receiver documenting the services the provider will furnish and defines the service standards the provider is obligated to meet.
Storage Configuration	Storage configuration pertains to selecting and setting up of the hardware and software environment in such a way that they can interoperate.
Storage Limitation Principle	This principle implies that the Personal data shall be stored in a way that permits identification of data subjects only for the period required to fulfil the purpose for which the data subject has provided their consent. In case the personal data has fulfilled the above purpose, it should be anonymized or erased from all information systems.
Supplier/Third Party	A natural or legal person, public entity, agency, or body other than the Data Subject, Data Controller, Data Processor, or authorized persons, involved in the processing of personal data
Use Case	Defined situation or scenario where a product or service could potentially be used.
Use Case Payback period	The payback period of the implemented use case
Use Case Return on Investment (ROI)	The ROI of the implemented use case

2. Policy Statement

2.1. Data Governance Office Domain

Objective: To set out a direction on the data governance office at MoH. The objective of the domain is to provide authority and control over the planning and implementation of the organization's Data Governance practices

Data Governance Office:

- Data Governance Head shall establish a Data Governance Office and identify and appoint relevant Data Governance working group roles.
- Chief Data Officer (CDO) shall approve both the Data Governance strategy and plan.
- The Data Governance Steering Committee shall appoint members to the data governance council.
- The Data Governance Council shall appoint members to the data governance working group

Data Governance Strategy & Plan:

- Data Governance Head shall establish a Data Governance strategy and develop a Data Governance Plan and align to MOH's overall Strategic Plan.
- Data Governance Head shall ensure that the appropriate resources and budgets exist to implement the Data Governance Program. Chief Data Officer (CDO) shall approve the same.
- Data Governance Head shall define and implement a governance structure to oversee rollout of the Data Governance Program. Chief Data Officer (CDO) shall approve the same.

Data Governance Domain Gap Analysis:

- Data Governance Compliance Manager shall conduct periodic Data Governance maturity assessment to identify gaps in the program.

Data Governance Training:

- Data Stewardship manager shall conduct Data Governance training and awareness sessions to relevant stakeholders across data domains.
- Data Privacy and Protection Manager shall conduct Personal Data Protection training

Data Governance Compliance, Audit Results and Monitoring:

- DG Compliance Manager shall establish Data Governance Compliance practices and document audit results and findings
- DG Compliance Manager shall monitor and ensure that MOH is complying with Data Governance Policy & Processes and DG Controls.
- Data Governance Compliance manager shall ensure compliance with local regulations.

Periodic Plan Review & Communications:

- DG Head shall conduct periodic reviews for the Data Governance Plan
- DG Stewardship Manager shall implement a communications capability to communicate updates on Data Governance activities and its effectiveness
- DG Compliance Manager shall establish a DG Compliance Monitoring process, which will include appropriate monitoring to allow Data Governance Programs to show compliance with the Data Governance policy and processes and align with local regulations at the appropriate points in their life cycles. MOH shall therefore set measurable objectives for its Data Governance Program.

Data Governance KPIs & Continuous Improvement:

- Data Governance Head shall establish key performance indicators (KPIs) on Data Governance domain. Data Steward shall gather statistics and define, implement and monitor continuous

improvement mechanisms for all Data Governance domains for his respective data domain. Chief Data Officer (CDO) shall approve the same.

Data Governance Approvals Register; Data Governance Issue Tracking Register & Version Control:

- Data Stewardship Manager shall document in a register all data governance decisions, tracking logs and implement a version control for data governance documents and artefacts

Escalation Management:

- The Escalation management shall be used to resolve Data Governance Issues which shall be handled according to the Data Governance Issue Management Process.
- SLAs be defined by data stewardship manager for issue resolution in agreement with all the MOH business functions
- In case of any delay in issue resolution as per the defined SLA, it shall be escalated based on the escalation matrix.

Roles and Responsibilities:

Chief Data Officer:

- Review and sign off on the Data Governance Strategy, and the Data Governance Plan.
- Ensure that the appropriate resources and budgets exist to implement the data governance program.
- Define and implement a Data Governance structure to oversee rollout of the Data Governance Program.
- Establish a Data Governance Office
- Resolve escalated issues raised from the Data Governance Council.

Data Governance Head:

- Identify and appoint relevant Data Governance roles under the guidance of CDE
- Resolve issues raised through DG Working Group or Data Stewardship Manager in escalation management, if not escalated further.
- Coordinate with the Chief Data Officer to develop the plan, identify the milestone, set Data Governance KPIs for DG Department.
- Chair the data governance working group

Data Stewardship Manager:

- Document in a register all data governance decisions, tracking logs and implement a version control for data governance documents and artefacts
- Resolve issues raised through escalation management in the DG working group.
- Conduct Data Governance trainings and awareness
- implement a communications capability to communicate updates on Governance activities and its effectiveness

DG Compliance Manager:

- Audit, monitor compliance and ensure that corrective actions are documented and implemented in case of deviation from the local regulations.
- Conduct periodic reviews for the Data Governance Plan
- Establish a DG Compliance Monitoring process, which shall include appropriate monitoring to allow Data Governance Programs to show compliance with the local regulations at the appropriate points in their life cycles.
- Shall conduct periodic Data Governance maturity assessment to identify gaps in the program

- Shall establish Data Governance Compliance Management practices and document audit results and findings.

Data Steward:

- Oversee implementation of data governance policies defined within their respective business domains. Help promote a culture of awareness of DG policies within their data domains.
- Identify the Issues related to their domain, and if not able to resolve escalate it according to Data governance issue management process

2.2. Data Catalog and Metadata Domain

Objective: To understand the large volumes of data and achieve a common understanding about its meaning, MoH must collect, maintain, manage business, technical and operational metadata and data lineage of data elements and associated processes.

Such practices would help to summarize information and describe characteristics of data in terms of definition, usage, source, structure, and transformations at various stages, thus ensuring transparency and traceability of data for current and future use.

Domain Details:
The domain provides necessary guidelines for creation & maintenance of Business metadata, Operational metadata, Technical metadata, and Data Lineage along with tool automation.

Policies in the following document are divided into 8 sections:

1. Add/modify business metadata
2. Add/modify technical metadata
3. Add/modify/ data lineage
4. Data catalog tool automation
5. Metadata access management
6. Performance management & monitoring
7. Metadata issues management
8. Training & awareness

Add/modify business metadata:

- Data Steward in consultation with the Metadata Manager shall be responsible for undertaking the creation/modification of business metadata of data elements by leveraging the defined business glossary process.
- Data Steward shall be responsible for data elements for their respective data domains.
- Data Stewardship shall be responsible for data elements of data domains common across organisation units along with data steward.
- Data custodian shall be informed of any changes made to the metadata of the data element.
- Data Steward in consultation with the Metadata Manager shall be responsible to define the required metadata values for each data element including the following:
    - Criticality of the CDEs to the business
    - Business and technical metadata for the identified CDEs
    - Datasets containing master/reference data.

- Transactional data in applications.
- Derived/ analytical information data in reports.

- Considerations shall be given to criticality of the data, number of users of the data, likelihood of re-use, and complexity of data for prioritizing the inclusion into the data catalog.
- The Data owner shall be accountable for approval of creation/ modification of business metadata and technical metadata of data elements of their respective data domain.
- The Data Steward shall capture the key attributes of business metadata pertaining to the data element and ensure it shall reflect the most current information.
- The Data Steward shall ensure that business metadata is version controlled using specific attributes to identify the version that they were captured against.

Add/modify technical metadata:

- Data Custodian in collaboration with the Metadata Manager shall undertake the creation/modification of technical metadata of data elements.
- The Data Custodian in collaboration with Metadata Manager shall be responsible to collect/update the technical metadata of the identified Data Elements:
  - Data Range, System name, Environment name, Schema name, Table name, Column name, Data type, Primary key, Foreign key
- The Data Custodian shall ensure that technical metadata is version controlled using specific attributes to identify the version that they were captured against.

Add/modify/ data lineage

- The Metadata Manager would be responsible for creating/updating data lineage between different sources of data by leveraging the defined data lineage process.
- Data Lineage of the CDEs of the organisation units shall be captured and published.
- Data Custodians shall be consulted by the metadata manager to analyse and create the data lineage information flow in the system.

Data catalog tool automation:

- Data Catalog tools shall be used to capture business glossary, technical metadata and data lineage of data elements and act as a central metadata repository.
- The Metadata Manager shall create a Data Catalog plan to manage the implementation of its Data Catalog and adopt a data catalog tool.
- Data Steward in consultation with the Metadata Manager shall identify CDE's and its corresponding sources to prioritize its coverage in the data catalog tool.
- Data Steward and Data Custodian shall register, populate and update the business glossary and technical metadata respectively within the Data Catalog. These shall be implemented as workflows in

the Data Catalog automated tool

- The Metadata Manager shall review on a regular basis the trust certificates assigned by users to the metadata within the Data Catalog as per Trust Certificate Review Process.
- The Metadata Manager shall maintain a data catalog tool activity log.
- The Metadata Manager shall ensure that the tool is updated to its latest version, in case of exception a release management strategy shall be maintained along with its rationale for exception

Metadata access management:

- Metadata Manager shall establish and follow Metadata Access Management process for the approval of connecting the Data Catalog tool to the MOH's Data Sources.
- Metadata Manager shall establish and follow Metadata Access Management process for providing its employees an access to the Data Catalog tool as per the Role-Based Access Control defined by the organisation.
- The Data Stewards shall work with organisation units to ensure that all the defined business glossary and technical metadata is accessible through a central data catalog tool.
- The Information Security Manager in collaboration with the metadata manager shall define access controls for sensitive metadata in accordance with Data Classification / Personal Data Protection domain (section 2.13 and 2.14).
- Data Owner shall approve and be accountable to implement the above access controls for sensitive metadata.
- Access to metadata values shall be restricted if it divulges information that is not for enterprise-wide consumption.
- Access to non-secured metadata shall be made easily available and encouraged.
- Accountability for appropriate usage of metadata by the organisation units shall be assigned to their respective Data Stewards

Performance management & monitoring:

- Data Stewardship Manager shall establish key performance indicators (KPIs) to gather statistics on the adoption of Data Catalog by users.
- The DG Compliance Manager, Metadata Manager, Data Stewardship Manager and Data Steward shall track the metrics periodically to monitor the progress of the quality of metadata and to ensure compliance to policies of Data Catalog and Metadata domain.
- The Metadata manager along with the Data Steward shall track the metrics periodically to monitor the progress of the quality of technical metadata.
- The Metadata manager shall establish KPIs to monitor the progress on data lineage, periodically.

- The Data Governance Compliance Manager shall collaborate with the Data Stewards and Data Custodians to define additional metrics, as needed, to track the quality of business glossary, metadata, and data lineage.

- The Data Governance Compliance Manager shall conduct periodic review of quality and completeness of business glossary, metadata and data lineage and record the observations of the reviews and rectify the corrections.

- The Metadata Manager shall develop and publish the Metrics/KPIs reports based on the metrics to the Data Owners and Data Governance Council.

Data Catalog and Metadata Issue Management Process:

- MOH shall leverage the defined data catalog and metadata issue management process for registering / escalating / resolving / remediating issues related to business glossary, technical metadata, and data lineage as per the data governance operating model.

- The process shall include reporting of identified business glossary, technical metadata and data lineage issues to the Metadata Manager and development of remediation actions within defined SLAs.

- The process shall be implemented as a workflow in the Data Catalog and Data Lineage automated tool.

Training & awareness:

- Metadata Manager shall deliver the Data Catalog training to its employees, to accelerate adoption, and increase its usage.
- Data Catalog training shall cover all the employees who directly need to discover, analyse or administer metadata or flow of data.

Roles and Responsibilities:

Data Stewards:

- Create or modify business metadata
- Define metadata for the critical data elements (CDEs)

Data Custodians:

- Create or modify technical metadata
- Support in data lineage creation

Metadata Manager:

- Manage the implementation of the data catalog tools
- Create required workflows in the data catalog tool
- Maintain an activity log for the data catalog tool
- Monitor data catalog & metadata KPIs
- Provide required training to MOH employees regarding data catalog & data lineage

Information Security Department:

- Define access controls for sensitive metadata

Data Owner:

- Provide approval to the business or technical metadata created or modified

2.3. Data Quality Domain

Objective: The objective of this domain is to provide guidelines for Data Quality Management of MoH's data.

Domain Details:
This DG domain covers managing data quality as an ongoing practice to improve availability of high-quality data across all channels, improve data usability and reduce time and expenses associated with excessive data reconciliation, and maximize business outcomes.
Policies for data quality domain are divided into 9 section as detailed below

1. Critical Data Elements Identification
2. Developing Data Quality Rules for applicable DQ dimensions
3. Data Quality Threshold determination
4. Data Profiling (Testing Point)
5. Data Cleansing
6. Data Quality Attribute Registration
7. Data Profiling (Test Execution)
8. Data Profiling (Scorecards)
9. Data Quality Issue Management
10. Data Quality Issue Remediation

Critical Data Elements Identification:

- The data attributes critical for business functions and processes shall be identified by Data Stewards in collaboration with data steward and Data Custodian for their respective data domain using the CDE Management Process.
- CDEs shall be documented in Data Catalogue.

Developing Data Quality Rules:

- Data Steward shall work with the respective Stewards & Data Custodian's to develop and maintain data quality rules for the identified Critical Data Elements to ensure availability of good quality data.
- Data Steward must ensure that Data Quality rules for CDEs are captured, documented, and approved. The CDE Management process shall be leveraged for defining the data quality rules for CDEs
- Business rules shall be developed using a data quality business rule/dimension framework.
- Data Quality rules are defined for each critical data element and the following Data Quality dimension shall be considered:

    - Completeness: It means that the required data is populated.
    - Conformity: It means that the data conforms and follows the business rule i.e. set of standard data definitions like data type, size and format
    - Uniqueness: It means that nothing shall be recorded more than once
    - Accuracy (Range): The rule describes the acceptable margin of error against reality to support the intended purpose(s) of the data.
    - Consistency: It means data across all systems reflects the same information and are in sync with each other across the enterprise.
    - Integrity: Integrity means validity of data across the relationships and ensures that all data in a database can be traced and connected to other data.

- Timeliness: The rule describes acceptable latency between data capture, use, transformation, reporting, and sharing.

- Entity shall use other dimensions as well based on the requirements.

Data quality threshold determination:

- Data stewards shall ensure that data quality threshold has been defined for each CDE for measuring Data Quality score of Data Domain and decide on the desired Metric for grading CDEs and monitor quality over time.
- Data Quality thresholds must be recorded in a centralized repository/Data Catalogue for future reference and maintenance.

Data Profiling (Testing Point):

- Data Steward are responsible for identifying the appropriate testing points where data shall be profiled.
- CDEs shall be profiled as close to their original source as possible to ensure that downstream consumers are receiving the highest quality data using the CDE Management process.

Data Quality Attribute Registration:

- The Data Owners shall confirm the successful listing and recording of CDE attributes.
- Access to attribute data must be controlled to protect CDEs.

Data Profiling (Test Execution):

- Test execution must be performed using approved tools as defined under Data Governance implementation.
- A standard minimum test execution frequency must be defined to ensure that test results can be aggregated and reported.
- Test execution shall be the shared responsibility of both the business and IT. It shall be facilitated by the Data Stewards

Data Profiling (Scorecards):

- Data Steward shall aggregate and publish the results of the data quality profiling efforts in a consistent manner.
- Results of data profiling shall be recorded using enterprise data quality metrics and established thresholds by the data steward.

Data Cleansing:

- Data cleansing shall be performed as part of the data integration exercise. Data steward in collaboration with Data Custodian shall cleanse the data covering the following activities -
- Unwanted observations from your dataset, including duplicate data objects or irrelevant observations shall be removed.
- Structural errors which are identified when MOH measures or transfers data and notices strange naming conventions, typos, or incorrect capitalization shall be fixed.
- Unwanted outliers in the analysed dataset shall be filtered.
- Missing values shall be handled by either entering missing values based on observations or altering the way the data is used to effectively navigate null values.
- Data quality assurance shall be performed to ensure that the data is cleaned as per the defined rules and standards.

Data Quality Issue Management:

- Data Steward must ensure that a standard data quality management process is established for effectively capturing, monitoring and prioritizing issues.

- Data Stewards must coordinate with stakeholders for effective monitoring of Data Quality Issues.

  - As part of the process, the data steward shall develop the capability to report, assign, prioritize and remediate Data Quality Issues.

Data Quality Issue Remediation:

- The Data Stewards shall partner with the Data Custodians to take necessary steps and define a timeline for remediating a Data Quality Issue.
- Remediation time shall be determined by the severity of the issue and criticality level of the impacted data. The severity level shall depend on the impact to the business.
- The proposed remediation end-date shall be monitored by the data quality management process for on-time implementation.

Roles and Responsibilities:

Data Steward:

- Support and ensure the implementation of Data Quality
- Provides supports in identification of CDEs and defining business rules
- Implement data quality rules on all Identified CDE's across dimensions
- Develop and execute the Data Quality rules using standard Data quality tool
- Ensure implementation and adoption of data quality policy & process in the respective data domain groups.
- Schedule periodic data quality rule jobs to continuously monitor Data Quality
- Perform RCA if the identifies issue is related DQ activities and ensure timely completion
- Provide inputs for Remediation Plan
- Review all Data Quality documents and provide sign offs

Data Custodian:

- Provide necessary access to the Data Steward for Data Profiling activities.
- Provide table column mapping for identifying CDE's
- Perform RCA if the identifies issue is related to Data/system
- Provide inputs for Remediation Plan
- Implement system/Data Fix

Data Stewardship Manager:

- Conducts periodic Data Quality maturity assessment to identify gaps in the program
- Monitors and ensures the program is progressing to schedule, and within its boundaries.
- Documents in a register all data governance decisions, tracking logs and implement a version control for data quality documents and artefacts
- Resolve issues raised through escalation management, if not escalate further.

2.4. Data Operations Domain

Objective:

The objective of this domain is to define the guidelines to manage the data lifecycle: from creation and initial storage to the time when it becomes obsolete and is deleted. The life cycle for data crosses different application systems, databases, and storage media. The cycle is made up of phases of activity including data acquisition, processing, storage, sharing, retention, archiving and purging.

Data Acquisition Activities:

- The Data Requester shall follow the data acquisition process to acquire data from legitimate sources.
- The data steward shall identify the requirements for data acquisition such as availability of data, existence of personal data and the authority to access the data.
- The Data Owner shall approve data acquisition before data is acquired for its respective data domain.
- In case there are multiple data owners involved, approval from all the data owners shall be required.
- The Data Steward, in consultation with the data owner, shall identify authoritative data sources for all datasets. The data steward shall ensure datasets are onboarded from their authoritative data sources (a system that contains registered data and is authorized to share that data with other systems).
- The data stewards shall ensure that all the CDEs created are formalized and recognized as per the Catalog and Metadata domain (section 2.2.).
- The data acquired shall adhere to data quality policies and processes.
- The data steward shall ensure minimal personal data is acquired and consent of the data subject is collected for the purpose of data use as per MOH's Data Privacy and Protection domain (section 2.14.).

Data Acquisition Logs:

- The data custodian shall create data acquisition logs and the data stewardship manager shall be accountable to maintain the logs to accurately document acquisition activities, and capture all relevant details associated with data collected

Data Maintenance:

- Each & every staff member shall be responsible to collect and maintain data as per their responsibilities in the Data Acquisition Process.
- The data stewardship manager, in collaboration with data steward, shall oversee that the data is collected and maintained in the manner and format prescribed by internal communications issued by MOH (such as Branch Circulars, Manual of Instructions, etc.).
- The relevant Data owner shall authorize any deviations from the communications.

Data Access:

- MOH shall ensure that data is classified as per the Data Classification Policy and access rights are implemented and authorization validated as per the Data Classification.
- The data steward, working with Data Custodian, shall ensure that the created / acquired data is complete / unaltered, and data is safe against unauthorized changes.
- The data owner shall specify the permissible additions / alterations which can be made to data after it is collected/created. The reasons for approving such changes must be clearly specified by the data owner.
- Any authorized additions / alterations must be explicitly shown and must be fully audited / traceable.

Service Level Agreement:

- The Data Steward shall create and share a Service Level Agreement template with relevant stakeholders. The data owner shall enter into Service Level Agreements on data to be acquired by the organization from external parties as per the data acquisition process.

Performance management & monitoring:

- The Data steward, in collaboration with Data Owner, shall establish and cement key performance indicators (KPIs) and their target levels to measure the performance of the data acquisition strategy. The KPIs, at the least, include the following metrics:
  - % of data acquisition requests completed
  - Volume of data created/acquired in a month

The DG Compliance Manager shall track and monitor the established Data Acquisition KPIs and publish the same to the Data Governance Head.

Data Processing:

Data Processing Activities:

- The data steward and data custodian shall ensure that all data processing is visible to the stakeholders in the form of data flows and Lineage, that is, Visualized data movement across the source and target with key processes.
- All transformations (such as changes in format or structure) from source to target shall be captured in the lineage and the operational metadata as per Data Catalog and Metadata domain (section 2.2.) (section: Add/modify data lineage)
- Classified data shall be processed by the data users as per the authorization and classification levels in the Data Classification domain (section 2.13.).
- MOH shall adhere to MOH Data Privacy and Protection domain (section 2.14.) for processing personal data. (See Data Privacy and Protection domain (section 2.14.).
- To demonstrate transparency & accountability, Data Privacy and Protection Manager store records of all its processing activities of personal data in the personal data protection register as per Data Privacy and Protection domain (section 2.14.).

Data Processing Architecture:

- Data Architect shall employ and document a Data Processing Architecture that has the capability for efficient processing of various data volumes, variety and velocity of data and optimizes data processing and systems performance as per the Data Architecture and Modelling domain (section 2.6.).
- The Architecture shall cover both real-time and batch processing operations.

Data Processing Systems:

- The data custodian, in consultation with the Data Architect, shall ensure relevant data processing systems are implemented for processing data.
- The data custodian and the demand and information management team shall leverage Online Transactional Processing (OLTP) systems to handle the management of transactional data.
- The data custodian, demand and information management team and AI and advanced Analytics team shall leverage Online Analytical Processing (OLAP) systems to handle aggregated historical data to enable large organizational datasets and access to analysis requests. OLAP shall respond to complex analytical queries such as reporting, forecasting, and so on.

Performance Management & Monitoring:

- The Data steward, in collaboration with Data Owner, shall establish and cement key performance indicators (KPIs) and their target levels to measure the performance of the data processing strategy. The KPIs should, at the least, include the following metrics:
    - Volume of data processed
    - # data processing activities

  The DG Compliance Manager shall track and monitor the established Data Processing KPIs and publish the same to the Data Governance Head.

Data Storage Plan & Forecasting:

- Data custodians, in consultation with the Enterprise Architect, shall conduct storage infrastructure utilization forecasts of MOH's information systems and servers to plan and budget future storage requirements of MOH.
- The forecast shall help MOH:
    - Predict future storage capacity needs
    - Estimate budget for future storage acquisitions.

Database Technology Assessment:

- The Data Architect shall assess and evaluate the current capabilities and future aspirations for selection of the Database Management System Software.
- The data custodian, in consultation with the Data Architect, shall ensure that the data in the database management system is stored throughout in an environment suited to its format and security classification (See Information Security Policy and Data Classification domain (section 2.13.), to ensure its preservation from harm or degradation and its security from loss or unauthorized access.
- The data custodian, in consultation with data steward, shall assess the requirements and capabilities of the database technology and mode of storage of data (such as primary/secondary/tertiary storage) and identify deficiencies in the storage of data to initiate a remediation plan for any deficiencies found.

Disaster Recovery and Business Continuity Plan:

- The data custodian shall establish and follow a clear strategy for the data backup.
- The data custodian shall work with the Business Continuity team to define and implement a Disaster Recovery Plan, aligned to MOH’s disaster recovery and business continuity strategy, policies and processes to mitigate risks in the event of system failure.

- The disaster recovery plan shall include a Business Continuity Plan, outlining how business shall continue operating during an unplanned disruption in service in the short and long term. Business Continuity Plan shall be approved by the Information Security Manager.
- The Data Stewardship Manager, in coordination with the Data Custodians, shall create a list of information systems ranked based on their business criticality and potential monetary and reputational losses because of emergency or disaster. The list shall be used to establish an order of systems recovery in the disaster recovery plan.

Database Management:

- The data custodian shall monitor and report database performance on a regular basis to the Data Architect.
- The data architect shall establish and follow a clear process for managing its Storage Configuration (Storage configuration process).
- The data architect shall have its DBMS tools updated to the latest published Vendor release or shall have a plan to update to the latest release & shall document the analysis and rationale If the latest release is not applicable to the MOH
- The data architect shall establish and implement database performance Service Level Agreements specifying the Entity's requirements for the database's performance, data availability and recovery. The Chief Architect shall approve the Service Level Agreement.
- The Data Architect shall establish and follow a clear process for the implementation of database changes from Testing to Production Environments (Database change process).

Data Security:

The applicable security protocols as per the guidelines from Information Security Policy shall be incorporated while storing the data residing within MOH.

Performance Management & Monitoring:

- The Data Architect, in collaboration with Data Custodians, shall establish and cement key performance indicators (KPIs) and their target levels to measure the performance of the data storage strategy. The KPIs, at the least, include the following metrics:

    - % of total data storage capacity used
    - % of data storage capacity used by type of database
    - % of data storage capacity used for backups
    - Number of performed data transactions
    - Average time of queries execution.

- The DG Compliance Manager shall track and monitor the established Data Storage KPIs and publish the same to the Data Governance Head.

Data Retention:

Retention Period:

- The data steward shall define and the Data Owner along with the Compliance Officer all approve the retention period of the different categories of the datasets stored by the organisation as per the

business and the regulatory requirements/ guidelines/ directions.

- The Data Custodian shall implement the Retention Periods for all data sets.
- Under no circumstances may a retention, retirement or disposal decision be made as a means to circumvent any rights of access (such as retaining data for a longer than required interval in a system to facilitate access) or other legal or regulatory requirements.
- Retention of data in no case be less than the period mandated by relevant regulation. Data steward and data owners shall consult the relevant regulators such as NDMO and NCA for retention periods.
- Records containing personal data (see the Data Privacy and Protection domain (section 2.14.)) be retained only for as long as it is necessary to retain them, considering the purpose for which they were created/collected and must be destroyed once it is no longer necessary to retain them unless mandated by law or there is a legal case.
- The data steward shall ensure that MOH's retention period is in line with the contractual agreements with data providers (e.g. MOH customers, employees, vendors, external organizations that participate in data sharing) from whom the data is sourced.
- The data stewards shall work with data custodians to ensure that only applicable data is retained in a cost-effective manner as per the requirements
- The data steward shall revisit the retention requirements and receive signoff from the data owner periodically.

Data Retention Preparation:

- The data steward shall prepare data for retention as per the Data Catalog and Metadata domain (section 2.2.) The data custodian shall ensure that data is retained in their relevant systems.
- The data steward shall manually or systematically label individual data sets in the data catalog upon data acquisition to help identify the data type and the data set's associated retention period.
- Data labels shall be manually or automatically updated by the data steward if there is a change in the retention period or classification of the data sets.
- The steward shall ensure that the retained data adheres to the Data Quality domain (section 2.3.) and processes.
- The data custodian shall determine the classification, access and sharing requirements for retained data (refer to Data Classification, Personal Data Protection and Data sharing and Interoperability domains (section 2.14., section 2.9.) & get the same approved by the data stewardship manager

Data Review:

- The data custodian shall undertake periodic or ad hoc reviews of retained data, particularly for higher risk categories of data (such as data classified as 'top secret' & 'secret'), when appropriate trigger events occur.
- The data custodian shall identify and document the gaps in current data retention practices with respect to the data retention policy.

Retention Register:

- The data steward shall maintain a register of all data tables and attributes that are retained.
- The steward shall label data at the time of placing records to facilitate easy location and handling of data.
- The data steward shall maintain and update the register with all details regularly. The data owner shall

review the register.

Performance management & monitoring:

- The Data Owner, in collaboration with Data Steward, shall establish and cement key performance indicators (KPIs) and their target levels to measure the performance of the data retention strategy. The KPIs, at the least, include the following metrics:
    - Volume of data retained
    - % (in volume) of data retained beyond retention period
    - Capacity - size of the unused storage
- The DG Compliance Manager shall track and monitor the established Data retention KPIs and publish the same to the Data Governance Head.

Data Archival:

Archival Period:

- The data steward, in consultation with the data owner, shall define the archival period of the datasets stored by the organisation as per the business requirements and the regulatory/ guideline/ directions.
- Under no circumstances may an archival decision be made as a means to circumvent any rights of access (such as archiving data for a longer than required interval in a system to facilitate access) or other legal or regulatory requirements.
- Archival of data in no case be less than the period mandated by relevant regulation. Data owners and data stewards shall consult the relevant regulators such as NDMO and NCA for archival periods.
- The data steward shall ensure that MOH's Archival Schedule is in line with the contractual agreements with data providers (e.g. MOH customers, employees, vendors, external organizations that participate in data sharing) from whom the data is sourced.
- The data custodians shall refer to the data archival and retention registers and review the retention and archival schedules to set up an automated data archival process to move the data sets that have exceeded the retention period into archives.
- The data custodians shall review the archival schedules and shall set up an automated data deletion process to move the data sets that have exceeded the archival period into the cool-off period, post completion of which the data sets shall be disposed of. Refer to the Data Deletion section for more details on the cool-off period.
- The archival requirements shall be revisited by the Data stewards in consultation with the data owners periodically.
- All records kept under archival be given serial reference/index number based on the number of years of storage required.

Data Retrieval:

- The data owner shall specify the circumstances (such as regulatory or legal requirement) under which archived data can be moved to the active stage.
- The data custodian shall move archived data sets to active usage, under these special circumstances.
- The data owner shall review and approve data retrieval requests for archived data on a case-by-case basis.

Archival Register:

- The data steward shall maintain registers for all data tables and attributes that are archived for future use with their archival, cool-off and disposal periods.
- The data steward shall maintain and update the register with all details regularly. The data owner shall review the register.

Audit Trail:

- The data custodian shall maintain an audit trail for data archival activities for archived datasets.
- The trail shall include at minimum the action (movement of data to archival, retrieval, cool off, etc.), time stamp when the action happened, action taker and action approver.
- The data custodians shall manage data change history, including archival and audit trail of the activities.
- The data stewards and data custodians shall determine the classification, sharing, and change requirements for archived data (refer to Data Classification domain (section 2.13.) and Personal Data Protection domain (section 2.14.))

Performance management & monitoring:

- The Data Owner, in collaboration with Data Steward, shall establish and cement key performance indicators (KPIs) and their target levels to measure the performance of the data archival strategy. The KPIs, at the least, include the following metrics:
    - Volume of data archived
    - % (in volume) of data archived beyond archival period
    - % (in volume) of data brought back from archives to active stage
- The DG Compliance Manager shall track and monitor the established Data Archival KPIs and publish the same to the Data Governance Head.

Data Deletion:

Deletion Period:

- The Data Steward, in collaboration with the Data Owner, shall define the disposition period of the datasets stored by the organization as per the requirements of the use cases supported by the datasets and the regulatory requirements/ guidelines/ directions.
- Under no circumstances may a disposal decision be made as a means to circumvent any rights of access (such as not disposing data when required to facilitate access to that data) or other legal or regulatory requirements.
- Records containing personal data (see Personal Data Protection domain (section 2.14.) for more details) shall be destroyed once it is no longer necessary to retain them unless mandated by law.
- The data steward shall ensure that MOH's Deletion Schedule is in line with the contractual agreements with data providers (e.g. MOH customers, employees, vendors, external organizations that participate in data sharing) from whom the data is sourced.

- The deletion requirements shall be revisited by the Data stewards in consultation with the data owners periodically

Data Disposal Technique:

- The data custodian shall ensure correct retirement and disposal techniques (such as data deletion, overwriting, degaussing, physical destruction, etc.) are employed.
- Data owner shall ensure that the data is no longer required (for work, evidence, support litigation etc.) before approving data deletion.
- The data custodian shall dispose data based on data archival and deletion period.
- All data deletions shall be approved by respective business owners prior to deletion.

Cool-off Period:

- The data custodian shall provide a cool-off period to the business before data is disposed of. The data steward shall gauge any operational impacts owing to non-availability of the data to be disposed of.
- The data custodian shall ensure that:
    - The data approaching its disposition schedule shall be retired to a secure offline or near-line repository (intermediate storage) for a cool-off period to ensure there is no operational impact
    - The data shall be disposed of once the cool-off period is complete.

Audit Trail:

- The data custodian shall maintain an audit trail for all data disposal activities for data that is disposed.
- The trail shall include at minimum the action (movement of data to cool off stage, deletion of data etc.), time stamp when the action happened, data disposal technique used, action taker and action approver.
- The data custodians shall manage data change history, including disposition and audit trail of the activities.

Performance Management & Monitoring:

- The Data Owner, in collaboration with Data Steward, shall establish and cement key performance indicators (KPIs) and their target levels to measure the performance of the data disposal strategy. The KPIs, at the least, include the following metrics:
    - Volume of data deleted
    - % (in volume) of datasets not disposed within period of disposition
- The DG Compliance Manager shall track and monitor the established Data Deletion KPIs and publish the same to the Data Governance Head.

Issue Management:

- The DG policy & procedure manager shall define a Data governance issue management process for registering / escalating / resolving / remediating issues related to data acquisition, data processing, data storage, data retention, data archival & data deletion as per the data governance operating model.

Roles & Responsibilities:

The following roles play an important part in governing data operations in MOH:

Data Steward:

- Ensures all relevant domains (such as Data quality, business glossary, data lineage, metadata management etc.) are adhered to throughout the data lifecycle.
- Defines data operations requirements and maintains acquisition and retention registers.
- Identifies authoritative data sources and ensures minimal personal data is collected.
- Ensures that the created / acquired data is complete / unaltered and safe against unauthorized changes.
- Defines data retention, archival and disposal period, and requirements for MOH.
- Oversees that data is collected and maintained in the manner and format prescribed by internal communications issued by MOH.
- Creates Service Level Agreements and Data Sharing Agreements for data sharing and acquisition.
- Supports to establishes key performance indicators (KPIs) and their target levels to measure the performance of data acquisition, processing, retention, archival and deletion strategies

Data Stewardship Manager:

- Maintains logs of data acquisition activities
- Oversees that the data is collected and maintained in the manner and format prescribed by internal MOH communications.
- Creates information system prioritization list to establish an order of systems recovery in disaster recovery plans.

Data Custodian:

- Creates Data Storage Plan and Forecasting, database technology assessment and performs database management.
- Ensures that all data processing is visible to the stakeholders in the form of data flows and Lineage.
- Ensures relevant data processing systems are implemented for processing data.
- Establishes and follows a clear strategy for the data backup.
- Monitors and reports database performance.

Data Architect:

- Employ and document a Data Processing Architecture with capability to process various data volumes, variety and velocity of data and optimize data processing and systems performance.
- Assess and evaluate the current capabilities and future aspirations for selection of the Database Management System Software.
- Establish and follow a clear process for managing its storage configuration and shall have the DBMS tools updated to the latest published Vendor release.
- Establish and implement database performance SLA specifying Entity's requirements for database's performance, data availability and recovery.
- Establish and follow process for implementation of database changes from Testing to Production Environments
- Establish key performance indicators (KPIs) and target levels to measure the performance of the data storage strategy in collaboration with Data Custodians

Data Owner:

- Enter into Service Level Agreements on data to be acquired by the organisation from external parties.
- Approve data acquisition, retention, archival and disposal requirements for data.
- Specify the permissible additions / alterations which can be made to data after it is collected/created and state reason.
- Establish and cement key performance indicators (KPIs) and their target levels to measure the performance of the data acquisition, data processing strategy, data retention strategy, data archival strategy in collaboration with Data Steward.
- Specify the circumstances (such as regulatory or legal requirement) under which archived data can be moved to the active stage.

2.5. Document and Content Management Domain

Objective: Document and Content Management domain requires plan, documents digitization and workflows managing the data lifecycle for documents. The domain would help MOH to focus on maintaining the integrity of and enabling access to documents and content stored outside of relational databases across the ministry.

Document and Content Management Plan:

- Data Stewardship Manager under the guidance of Data Governance Head shall create a Document and Content Management Plan to implement and control activities aiming to manage the MOH's documents and content lifecycle.
- Data Governance Head shall collaborate with Data Governance Council members to finalise and approve Document and Content Management plan.
- Data Stewardship Manager shall perform following activities-
  - Review its current requirement and usage of documents and the supporting document management capabilities
  - Establish a plan to standardize document formats, describe documents using appropriate metadata
  - Manage the storage and access to documents using a repository.

Document's Naming Convention:

- Data Steward shall define and Data Stewardship Manager shall ensure the Documents' naming conventions are followed across MOH.
- Naming Convention shall be established before MOH organisation units begin collecting files or data in order to prevent a backlog of unorganized content that shall lead to misplaced or lost data.

Digitization Plan:

- MOH shall implement initiatives focused on eliminating the creation of paper-based documents in the MOH and replacing them with electronic documents.
- Data Steward in collaboration with Data Custodian shall create a Documents and Content Digitisation Plan to manage the implementation of paperless management initiatives.

Documents Prioritization:

- Data Stewardship Manager with collaboration of Data Steward shall identify and prioritize its documents to be stored and managed in its DMS. The result of the prioritization shall be a ranked list of documents to be used as an input in the implementation of the MOH's DMS.
- Documentations to be considered as high priority are legal or tax documents, Critical Business process documents, audit artefacts of the organization or customers

Workflows Management:

- Data Stewardship Manager with the collaboration of Data Steward shall design document and content management processes and Data Custodian shall implement corresponding workflows in DMS.
- All the prioritized documents shall be managed as per the documents and content management process and workflows.
- MOH shall introduce workflow tools (DMS) to support business processes, documents, assign work tasks, track status, and create audit trails. The workflow management shall provide for review and approval of content before it is published.

Training and Awareness:

- Data Stewardship Manager shall conduct the Document and Content Management training for the MOH's employees to increase the awareness on leading practices in the Document and Content Management.

Operations:
MOH shall implement appropriate controls mentioned in the Data Operations Controls document to be monitored across all document and content lifecycle stages.

Backup and Recovery:
- Data Custodian shall include the Document Management Systems within its overall backup and recovery plan. Data Owner shall be involved in risk mitigation and business continuity planning, to ensure these activities account for the security for vital records.

Retention and Disposal:
- Data Stewardship Manager shall establish and follow a clear document and content management process for retention and disposal of the MOH's documents. The process shall implement the MOH's data retention and disposal section mentioned in data operations policy.
- Data Privacy and Protection Manager shall periodically oversee the document privacy and security classification requirements and take actions to prevent loss, breach of documents as mentioned in the Personal data protection domain (section 2.14.).

Document Change Management and version Control:
- Data Stewardship Manager shall establish document change management to keep consistency, quality, and compliance of the documents in check. Data Stewardship Manager shall also define and implement version control for data management documents and artefacts that the Entity is the creator of.
- Document Change Control Process helps to reduce the errors in the critical documents and avoid the inconsistent flow of information, if the person at duty changes.

Access Approval:
- MOH shall consider ISD's Data Access Policy to establish and follow a document and content access process for providing MOH's employees access to documents and content stored in the MOH's Document Management Systems. Please refer to the Data Access Section in the Data Sharing & interoperability domain (section 2.9.).

Documents and Content Management Tools:
- Data Custodian shall implement tools supporting automation of the MOH's Document and Content Management.
- Data Custodian shall implement tools which shall be able to capture, store and manage documents in an electronic format, store and manage website content used by the MOH's portals and internet sites and provide users with a platform to collaborate real-time on electronic documents, communicate using chat and track changes in the documents.

- The tools shall include, at minimum, the following:

    - Document Management System -

An application used to capture, store, and manage documents in an electronic format (electronic documents and digital media). The selected DMS tool shall provide, at minimum, the following capabilities-

a. Storage of documents
b. OCR (Optical Character Recognition) functionality to analyse imported images
c. Indexing of documents
d. Versioning of documents including tracking of the history of changes
e. Secured access to documents
f. Global search and discovery on the registered documents
g. Document's workflows development

- Web Content Management System - An application used to store and manage website Content used by the MOH's portals and internet sites

Collaboration tools - applications providing users with platform to collaborate real-time on electronic documents, communicate using chat and track changes in the documents

KPIs:

- Data Stewardship Manager shall define key performance indicators (KPIs) and get it approved from the Data Governance Head established to measure its document management efficiency. The Data Stewardship manager shall develop KPIs at the strategic and operational levels and both quantitative and qualitative measures to review organizational performance against its goals.

Service Level Agreement:

- Data Stewardship Manager shall create and share a Service Level Agreements template with relevant stakeholders.
- MOH shall enter into Service Level Agreements (SLA) with document management service providers to operate the document and content management services.

Roles & Responsibilities:

Data Stewardship Manager:

- Create a Document and Content Management Plan aiming to manage the MOH's documents and content lifecycle under the guidance of Data Governance Head
- Review its current requirements, usage of documents and the supporting document management capabilities
- Establish a plan to standardize document formats, describe documents using appropriate metadata
- Manage the storage and access to documents using a repository.
- Conduct the Document and Content Management training for the MOH's employees
- Design document and content management processes and implement corresponding workflows in DMS.
- Define key performance indicators (KPIs) and get it approved from the Data Governance Head established to measure its document management efficiency.
- Create and share a Service Level Agreements template with relevant stakeholders.

Data Steward:

- Identify and prioritize its documents to be stored and managed in its DMS.
- Create a Documents and Content Digitisation Plan to manage the implementation of paperless management initiatives.

Data Custodian:

- In collaboration with Data Steward create a Documents and Content Digitization Plan to manage the implementation of paperless management initiatives.
- Include the Document Management Systems within its overall backup and recovery plan.

Data Owner:

- Participate in risk mitigation and business continuity planning, to ensure these activities account for the security for vital records.

Data Privacy and Protection Manager:

- Periodically oversee the document privacy and security classifications requirements.

Metadata Manager:

- Define requirements to collect metadata for MOH documents and content stored within the MOH's Document Management Systems in the MOH's Data Catalog automated tool.

Data Governance Head:

- Collaborate with Data Governance Council members to finalise and approve Document and Content Management plan.
- Enter into Service Level Agreements (SLA) to agree service provision and capacity levels with responsibility for operating the document and content management services.

The details of the respective roles and their responsibilities can be found in the data governance target operating model that has been defined for MOH.

2.6. Data Architecture and Modelling Domain

Objective:
To clearly set out a direction on data architecture and modelling. The purpose is to focus on the establishment of formal data structures and data flow channels to enable end to end data processing across and within MOH.

Domain Detail:

Baseline Data Architecture:

- The Data Architect shall develop baseline data architectures for information systems and components under their control, and a baseline enterprise data architecture across all key systems.
- The Data Architect shall develop and execute a plan to ensure full coverage of all systems that shall include:
    - Initial baseline data architecture production of all information systems controlled and maintained by MOH
    - Baseline Enterprise Data Architecture, covering the high-level architectural view across MOH's core systems, including systems not directly under the MOH's control.

- Data Architect shall include the following elements while developing the baseline data architecture deliverables:
    - The business and technical requirements that the data architecture supports, and those that are not currently supported by the data architecture
    - Identification of technical data architecture themes (for example, service-based/batch processing/data silos/data integration)
- Data Architect shall get the baseline architecture reviewed at the appropriate points in the system development life cycle by the Chief Architect or Data Governance Council.

Target Data Architecture:

- The Data Architect shall produce target enterprise data architecture. The completion of baseline data architecture is not a prerequisite for development of target enterprise data architecture but may be informed by it.
- The Data Governance Council shall provide consideration and justification to the data architect in appropriate time to produce the target enterprise data architecture.
- The target enterprise data architecture shall be a continuously evolving set of deliverables, reacting to external factors such as technology changes, business requirements and external factors.
- Data Governance Council shall ensure that the target enterprise data architecture is maintained as information systems and components are implemented, revised, or decommissioned.
- Data Architect shall produce target data architectures for information systems as they go through natural change cycles.
- The target data architecture shall influence technology and data requirements for system changes, in addition to the standard business and quality (non-functional) requirements.
- The target architecture must adopt established frameworks such as TOGAF, Zachmann etc.

Enterprise Data Architecture Categorization:

- The Data Architect shall classify architectural elements such as applications, databases, and information systems according to the following categories:

- **Emerging** – components that are a yet to be proven in a live environment; these components are likely to require proof of concept development, or collaboration through working groups to assess suitability
- **Current** – suitable components that are in development or deployment
- **Strategic** – components that are expected to be available in the medium term e.g. big data technologies, mobile apps, or other components that are anticipated to provide strategic advantage to the MOH's operation.
- **Retirement** – components that no longer help the MOH meet its strategic goals, and that are due to be decommissioned, replaced, or archived

Enterprise Data Architecture Standards:

- Data Architect shall use data architecture standards while designing, documenting, and developing data architecture or model. Data Architect Shall consider:
  - Statistical Data Standards
  - Geospatial Data Standards

Enterprise Data Modelling & Design:

- The Data Architect shall ensure the data model for core systems, enterprise data warehouse and data lake within the software development lifecycle are reviewed by the Chief Architect.
- Data models shall form a core deliverable of any system built, purchased, or commissioned by MOH as part of developing its data architectures in support of business and technology requirements.

Enterprise Data Modelling & Design - Implement Tools and Methods:

- MOH shall implement data modelling tools with the following minimum capabilities:
  - The creation of UML compliant models
  - Support for UML model interchange using the XMI Interchange Format
  - Modelling unstructured datasets
  - Associating metadata to models to facilitate and promote re-use
  - Model versioning and traceability

- Where MOH already has data modelling tools, it shall certify that any existing toolset meets the minimum capabilities. Evidence shall be captured and be available upon request to support any specification and development of centralised tooling.
- If MOH's toolset does not meet the requirements, MOH shall begin an initiative to fill the requirement gaps, whether that be through the purchase of new tooling or through other development or with help of suppliers.

Data Modelling Artefacts:

- The Data Architect shall use UML diagrams as the primary modelling notation throughout the software development lifecycle.
- Exceptions to the UML modelling standard shall be documented and submitted for authorisation by the Data Governance Council
- Data Architect along with Data Steward shall use models best suited to communicate with business stakeholders. For these purposes more, common tools such as text-based documents, presentation slides and spreadsheets shall be used.
- Data Governance Council shall ensure appropriate and effective communication to its departments and stakeholders.
- Data Architect shall use Entity-Relationship diagrams and Class Diagrams to document the structure and relationships of data objects at a conceptual, logical and physical level.
- Data Architect shall use Data Flow Diagrams to model the movement of data within and between the system, focusing in particular on data in MOH.

- Large data models data architect be subdivided into smaller subject area-based models to maintain clarity. Data models data architect fulfil the purpose of aiding understanding.
- Chief Architect along with Data Architect shall ensure that the following rules are adhered to when designing new conceptual data models:
    - Data objects are represented by nouns
    - Data relationships are represented by verbs
- Chief Architect along with Data architect shall ensure that the appropriate data type shall be used for attributes within tables when designing new logical data models. This shall also consider performance, storage, and data requirements.

- Chief Architect along with Data architect shall ensure that the following rules are adhered to when designing new physical data models:

    - Reference data tables shall have a primary key
    - Tables that use reference data tables shall use the reference table's primary key in the foreign key relationship
    - Reference data tables shall have, at a minimum, a primary key and a code value.

- Physical data types that have a length or precision specifier shall have an appropriate length or precision specified, and not left to the default value.
- Data Architect shall publish data models for reference and re-use within MOH. Data Architect shall be responsible for evaluating other pre-existing data models, and aligning or re-using data models for new systems where possible.
- Data Architect shall provide justifications in the system design where evaluating other pre-existing data models, and aligning or re-using data models for new systems is not possible. The Data Governance Council shall approve the same.

Enterprise Data Architecture and Data Modelling Deliverables:

Data Architect shall design, document and develop all the deliverables for including both data Modelling and Data Architecture.

The deliverables shall include the following:

Data Modelling Deliverable:

- Enterprise Data Model – A combination of Conceptual Data Models, Logical Data Models and Physical Data Models describing the data its relationships that are core to MOH's function
- Conceptual Data Model – Shall capture the high-level conceptual relationships and themes within the data and shall be used for business users to understand
- Logical Data Model – Shall capture the system independent tables, fields, and relationships and shall be used to aid development discussions
- Physical Data Model – Shall capture the specific implementation details and shall be used to implement and support systems, and to understand technical change
- Data Flow Diagrams – Shall cover data flows within and between systems and exist at multiple levels of detail.
- Data lifecycle model – Shall showcase lifecycle encompassing creation, utilization, sharing, storage, and deletion stages within the systems.
- Data model change process – Shall capture the change process required in order to change data profiles where a deliverable is deemed to be not required, justification shall be given by Data Architect and approved by Chief Architect.

Data Architecture Deliverable:

- Component model – Shall capture the technology components that make up the data architecture e.g. Master Data Management/Reference Data Management, Enterprise Service Bus (ESB), ETL tools, and how they relate to specific applications or technology systems
- Data security compliance design – Shall capture the key security touchpoints and tools and technologies used to implement security solutions.
- Data Architect shall refer to data dictionary and business glossaries to ensure consistency of terminology in architecture and model development.
- Data Architecture and modelling deliverables shall be considered to be produced for any data and analytics related initiatives, project and program. It shall be considered for the following systems also -
    - Data security and privacy systems
    - External - Open data management systems
    - Document and content management, or workflow systems
    - Systems for extract, transform, load (where they do not form an architectural component of another system)
    - Data warehouse, business intelligence and analytics systems
    - Line-of-business management systems, such as ERP, CRM, Spatial data, Statistical management, and other specialist information systems appropriate to MOH

Conceptual Data Model:

- Data Architect shall develop conceptual data models to support the architecture, development, and operational processes for its data.
- Conceptual data models shall be required as part of the system development life cycle and provided to the Chief architect or Data Governance Council through the Data Architecture Checkpoint as defined in controls
- Data steward shall engage with stakeholders, or otherwise undertaking business in the functional analysis and requirements gathering to understand all relevant business concepts and requirements
- Conceptual data modelling shall be performed at a system level (or group of information systems with similar concerns), or as part of Enterprise Data Modelling.
- Conceptual data models shall be used to provide documentation to support development of logical data models, change requests, impact assessments, and/or gap analyses between baseline and target state requirements

Logical Data Model:

- Logical modelling of relationships between entities (entity relationship diagram) shall describe referential integrity and normalisation concerns, unless the design relates to multi-dimensional information systems, such as data warehouses.
- Where data is de-normalised for performance or other reasons, Data Architect along with Data Steward shall ensure that this is documented, justified and approved by the Chief Architect
- Logical data models shall be independent of technical implementation details.
- Logical data models shall be used to provide documentation to support development of the physical data model, change requests, impact assessments, and/or gap analyses between baseline and target state requirements.

Physical Data Model:

- Data Architect shall develop physical data models for system designs and architectures that are based on the logical data models.

- A physical data model shall provide the detailed technical implementation specifications that represent the application and/or data repository perspectives of the data.
- Data Architect shall develop a physical data model that is used to support technical implementation and system operational functions.
- Data Custodian with the help of Data Architect shall provide a mapping between the logical data model and the resulting physical design to describe the implementation decisions involved.
- Data Architect shall highlight the dependencies that emerge as a result of using the embedded features of a tool.
- Physical data models shall be linked back to their logical models.

Roles & Responsibilities:

Data Architect:

- Develop baseline data architectures for information systems and components under their control, and a baseline enterprise data architecture across all key systems.
- Produce target enterprise data architecture. The completion of baseline data architecture is not a prerequisite for development of target enterprise data architecture but may be informed by it.
- Classify architectural elements such as applications, databases and information systems
- Use data architecture standards while designing, documenting and developing data architecture or model.
- Ensure the data model for core systems within the software development lifecycle are reviewed by the Chief Architect.
- Develop conceptual data models to support the architecture, development and operational processes for its data.
- Provide a standard business vocabulary for data and components
- Align Data Architecture with enterprise strategy and business architecture
- Data Architects provide enterprise data requirements for individual projects.
- Design reviews ensure that conceptual, logical, and physical data models are consistent with architecture and in support of long-term organizational strategy.
- Ensures that business rules in the applications along the data flow are consistent and traceable.
- Replication is a common way to improve application performance and make data more readily available, but it can also create inconsistencies in the data.
- Data Architect works with Enterprise Architects to manage data technology versions, patches, and policies each application uses, as a roadmap for data technology.

Data Stewards:

- Perform remediation, identify gaps in baseline vs target architecture and improve the overall process.
- Engage with stakeholders, or otherwise undertake business functional analysis and requirements gathering to understand all relevant business concepts and requirements, in conceptual data models.
- Ensure along with data architects that the documentation required in the Data Architecture and Modelling domain is completed.

Chief Architect:

- Translate the existing and upcoming business requirements into technical requirements. To help define the process, roadmap, conceptual design which cater to the project/initiative implementation requirements.
- Ensure that the rules are adhered to when designing new conceptual data models, new logical data models and new physical data models.

2.7. Reference and Master Data Management Domain

Objective: To clearly set out a direction on reference & master data management. The objective of the domain is to link all critical data to a single master file, providing a common point of reference for all critical data and lay down the requirements for reference & master data objects at MOH.

Domain Detail:

Define Master Data Domains, Reference & Master Data Drivers and Requirements:

- Data Stewardship Manager shall prioritize Master Data efforts based on business needs. Business needs include improved customer services; cost / benefit of proposed improvements.
- Data Stewardship Manager shall prioritize the reference data that improves data quality by standardization and increases operational efficiency.

Identify and Assess Data Sources:

- Data Custodian shall identify and prioritise the data Sources that have greater trust within MOH based on dimension defined in Data Quality domain (section 2.3.).
- Data Steward shall consider the data sources that are core and critical to day-to-day operations of the organization for upstream applications for Master Data Hub.
- The defined Reference & Master data management process shall be leveraged for finalizing the data domains for creating, modifying & archiving reference & master data in MOH

Define and document technical and business Match, Merge & De-merge Rules:

- Data Steward shall define and document technical and business Match, Merge & De-merge rules and Data Owner shall approve it.
- Data Steward shall document and define workflows based on the business and technical requirements.
- Data Custodian shall document end-to-end Source to Target Mapping of reference & master data attributes.
- Data Custodian shall also share the RMD requirement, data domain and source to target mapping with Data Architect.

Design Master & Reference Data Model:

- Data Architect shall define and design a logical and canonical master data model including the subject areas within the master data hub.
- Data Steward shall establish relationships between the codes, values, and description in reference data.

Define Architecture Approach for Implementation:

- Data Architect shall define the architectural approach to master data management as per Data Architecture and Modelling domain (section 2.6.), platforms of existing data sources, number of data sources, type of data, data volume and data consumption. Data architects may also consider the lineage and volatility, and the implications of high or low latency.
- Data Architect shall evaluate reference and master data management tools based on both business requirements and architecture options.
- Data Architect shall accommodate master and reference data relationships & affiliations as well as data hierarchies during architecture design & data flow design.
- Data Steward shall standardize and define reference and master data clearly.

Master Data Maintenance:

- Data Steward shall continuously monitor, review, and improve Master and Reference Data Objects.
- Data Steward shall share Reference and Master Data object change request with Data Owner for approval.

Roles & Responsibilities:

Data Stewardship Manager:

- Prioritize Master Data efforts based on business needs.
- Prioritize the reference data that improves data quality by standardization and increases operational efficiency.

Data Architect:

- Define and design a logical and canonical master data model including the subject areas within the master data hub.
- define the architectural approach to master data management as per Data Architecture and Modelling Policy, platforms of existing data sources, number of data sources, type of data, data volume and data consumption.
- Evaluate reference and master data management tools based on both business requirements and architecture options.
- Data Architect shall accommodate master and reference data relationships & affiliations as well as data hierarchies during architecture design & data flow design.

Data Steward:

- Consider the data sources that are core and critical to day-to-day operations of the organization for upstream applications for Master Data Hub.
- Define and document technical and business Match, Merge & De-merge rules and Data Owner shall approve it.
- Document and define workflows based on the business and technical requirements
- Establish relationships between the codes, values, and description in reference data.
- Standardize and define reference and master data clearly.
- Continuously monitor, review, and improve Master and Reference Data Objects.
- Share Reference and Master Data object change request with Data Owner for approval.

Data Owner:

- Approve technical and business Match, Merge & De-merge rules.

Data Custodian:

- Identify and prioritise the data Sources that have greater trust within MOH based on dimension defined in MOH Data Quality domain (section 2.3.)
- document end-to-end Source to Target Mapping of reference & master data attributes.
- Data Custodian shall also share the RMD requirement, data domain and source to target mapping with Data Architect.

2.8. Business Intelligence and Analytics Domain

Objective:

Aims to create & foster a culture of data-driven decision making in MOH, using advanced Artificial Intelligence (AI) & Analytics & BI technologies. The domain would help MOH generate valuable insights from its data so that the same can be used to drive innovation, create competitive advantage & also bring about cost & operational efficiencies across the ministry.

Domain Detail:

BI & Analytics Planning:

- The head of the AI & Advanced Analytics team in MOH & the head of demand & information management team data architect create a Business Intelligence (BI) & Analytics plan for MOH to manage & orchestrate the BI & Analytics program in MOH.
- As part of the plan, the head of AI & Advanced Analytics shall define the roadmap & identify resources related to AI & Advanced analytics use cases, whereas the head of demand & information management shall do the same for BI use cases.
- The plan shall be reviewed & updated periodically to ensure that it is aligned to MOH's business goals.

BI & Analytics Use Case Development Lifecycle:

MOH shall develop BI & Analytics use cases to support its tactical, strategic & operational business decisions, & store the underlying data required for these use cases in a centralized data platform.

The use case development lifecycle data architect consists of the following 4 phases:

1. Use Case identification
2. Use Case Detailing
3. Use Case Implementation
4. Use Case Validation

Use Case Identification:

- MOH shall identify & shortlist AI & Advanced Analytics use cases for MOH based on MOH's defined use case identification process.
- The head of the AI & Advanced Analytics team (along with the MOH demand manager) data architect prioritize the AI & Analytics use cases based on the business value & complexity of the use case
- The shortlisted & prioritized use cases data architect be signed off by the head of the AI & Advanced Analytics team & documented in a BI & Analytics register.
- The use case identification process data architect be repeated periodically to identify any new AI & Advanced Analytics initiatives
- MOH shall identify BI use cases by following the defined demand management request process
- The demand & information management team shall perform the initial requirement analysis for the BI use cases with business users & approve or reject the use cases accordingly

Use Case Detailing:

- The MOH head of the AI & Advanced Analytics team (in collaboration with data stewards) shall capture all the required metadata for the shortlisted AI & Advanced Analytics use cases so that the same can be used to create the use case implementation plan & validation criteria.

- The demand & information management team shall capture all the required metadata for the shortlisted BI use cases & provide the required test scenarios for validating the use cases

Use Case Implementation:

- The MOH AI & Advanced analytics team shall create an implementation plan for the shortlisted AI & Advanced analytics use cases, which shall be approved by the head of the AI & Advanced Analytics team & the business user.
- The MOH AI & Advanced analytics team shall decide if an exploratory POC implementation is required prior to the actual development of the AI & Advanced Analytics use case. If required, the POC shall be implemented by leveraging the POC use case ideation & development process
- In case the developed POC is approved, the AI use case shall be operationalized & deployed in production using the defined POC Industrialization & impact assessment process
- The use cases shall be developed using the latest AI & Analytics techniques leveraged by MOH.
- MOH shall leverage advanced Artificial Intelligence & Machine learning (AI & ML) capabilities & use batch/near real time/real time data depending on the use case requirements for implementing the AI & Advanced Analytics use cases wherever needed.
- MOH shall ensure that the use case implementation uses appropriate architectural components as stated in the Architecture & Modelling domain (section 2.6.)
- The MOH AI & Advanced Analytics team shall verify with data stewards on whether data subject consent has been provided for any personal data processed as part of the use case
- MOH shall not process any personal data as part of a use case beyond the validation period of the consent provided by data subjects
- The demand & information management team shall create the Functional Design Document (FDD) for developing the BI use cases.
- The data solutions delivery team shall develop the BI use cases as per the defined Report Request (Major & Minor) process
- The demand & information management team shall perform any required QA validation prior to the deployment of the BI use cases

Use Case Validation:

- MOH shall validate the use cases periodically as per their individual validation frequencies specified in their details.
- The MOH head of the AI & Advanced Analytics team (in collaboration with the MOH AI & Advanced analytics team) shall create a plan to validate the implemented AI & Advanced Analytics use cases to assess whether they provide the required ROI & fulfil needed business requirements.
- MOH shall leverage the POC industrialization & impact assessment process wherever possible to validate the implemented AI & Advanced Analytics use case
- The head of demand & information management shall create the plan to validate the BI use cases to assess whether they provide the required ROI & fulfil needed business requirements
- The validation results & gaps identified shall be approved by the business user & documented in the BI & Analytics register.

BI & Analytics Training & Awareness:

BI & Analytics Training:

- The MOH AI & Advanced analytics team & demand & information management team shall conduct joint training programs for all MOH departments, followed by an assessment periodically to upskill MOH employees in BI & Analytics capabilities.
- The training curriculum shall be updated periodically & validated by the MOH head of the AI & Advanced Analytics team & the head of the demand & information management team.
- The team shall document the percentage of employees involved in BI & Analytics initiatives in MOH who are trained in BI capabilities & their corresponding skills acquired.
- MOH employees shall leverage the acquired skills to independently create self-service reports, perform data analysis & create analytical data models wherever possible.

BI & Analytics Awareness:

- The data stewards (in collaboration with the head of the AI & Advanced Analytics team & demand & information management team) shall hold BI & Analytics awareness campaigns for their respective departments periodically to promote the adoption of BI & Advanced Analytics capabilities.

BI & Analytics Performance Management:

- The head of the AI & Advanced Analytics team & demand & information management team shall be jointly responsible for defining the KPI targets for the BI & Analytics program & monitoring the same on a periodic basis.
- The defined KPIs shall be published to the data governance council & signed off by MOH's Chief Data Officer.

Roles & Responsibilities:

Data Stewards:

- Identify the BI & Analytics use cases
- Define KPIs & acceptance criteria for the use case

AI & Advanced Analytics Team:

- Create a POC (if required) prior to developing the use case
- Develop AI & Advanced Analytics use cases

AI & Advanced Analytics Team head:

- Create the AI & Advanced Analytics plan
- Review & provide sign-off to any use case POC created
- Create a plan to validate the use cases

Demand & Information Management Team:

- Identification & validation of use cases related to BI
- Create FDD for the BI use cases

Head of Demand & Information Management:

- Create the plan for the creation of BI use cases

2.9. Data Sharing and Interoperability Domain

Objective: The objective of this domain is to provide policy to share the MOH's datasets appropriately in line with regulatory requirements & also to ensure a standardized exchange of data between its data assets and protect MOH's data from unauthorized access.

Domain Details:
MOH shall enable a standardized exchange of data between its various data stores, systems & applications & also among external entities through the data sharing & interoperability policies mentioned below.
The domain is divided into the following 11 sections within the two broad topics of data sharing & data interoperability:

1. Data Sharing & Interoperability Plan
2. Data Integration Solution Development Lifecycle
3. Integration Layer Operationalization
4. Data Sharing Policy Statements
5. Data Sharing Training
6. Monitoring & Compliance
7. Roles & Responsibilities

Data Sharing & Interoperability Plan:

- MOH shall assess its current architectural landscape to understand the consumption & exchange of data between its IT systems & identify pain points with respect to the format, context, contents & processing speed of such data exchange. It shall then define the target integration architecture & also create an implementation plan to achieve the same.

Data Integration Initial Assessment:

- The MOH data integration SME(s) (along with the individual data custodians) shall conduct an initial data integration assessment for identifying the challenges in the movement of data between systems, performing data discovery & documenting data lineage
- The results of the assessment shall be documented & signed off by the data integration SME

Target Data Integration Architecture:

- The MOH data integration SME(s) (in collaboration with the MOH Strategy & Data Architecture team & data custodians) shall design a target data integration architecture to meet MOH's data integration requirements & identified pain points.
- The target integration architecture shall be designed according to common integration patterns & shall favour the use of one-way integration patterns (e.g. request/response, broadcast, etc.) wherever possible for data sharing with other systems
- The data integration SME(s) shall re-use as many data integration & interoperability components as possible while designing the target architecture
- The target integration architecture shall be approved by the MOH data integration SME before its operationalization.

Data Integration Plan:

- The MOH data integration SME(s) (in collaboration with the Data Architect & data custodians) shall create a data integration plan to determine the activities, timeline & resources required for the

implementation of the target data integration architecture.

- The plan shall be approved by the MOH data integration SME & reviewed & updated (if required) periodically.

Data Integration Solution Development Lifecycle:

The MOH data integration SME(s) (in collaboration with the MOH Data Architect & data custodians) shall develop a data integration solution/layer that meets MOH's business needs & facilitates connection between its internal & external information systems.

The data integration solution development lifecycle shall cover the following 6 phases:

1. Integration Requirement & Design documentation
2. ETL & ELT Process Design
3. Integration Solution Development
4. Integration solution Testing
5. Integration Solution Deployment
6. Monitoring & Maintenance

Integration Requirement & Design documentation:

The MOH data integration SME shall be responsible for creating & maintaining the below documents to ensure a smooth implementation & traceability of the data integration program:

- **Integration Requirements Document:** This document shall provide details of the integration requirements, scope & implementation timeline
- **Solution Design Document:**
  This document shall contain details of the MOH target data integration architecture & data flow diagram
- The data integration SME shall review these documents periodically & update wherein required.

ETL & ELT Process Design:

MOH shall leverage the below defined processes for loading data in a centralized platform from multiple data sources:

1. **Extract, Transform & Load (ETL) Process** to load data from various sources into a data warehouse
2. **Extract, Load & Transform (ELT) Process** to load big data or unstructured data into a data lake in its raw format
   - ETL process shall be considered for loading structured data into the data warehouse. ELT process shall be considered whenever there is a large amount of unstructured involved that should be loaded into a data lake.
   - The above processes shall be reviewed periodically by the data integration SME & updated wherein necessary

Integration Solution Development:

- MOH shall develop the integration solution/layer as per the instructions provided in the integration plan & integration design documents
- The technical, business & operational metadata for the developed integration solution shall be documented & maintained by the data integration SME (please refer to MOH data catalog & metadata policy)

Integration Solution Testing:

- The MOH data integration SME (along with the data architect) shall test any changes to its developed integration solution before it is deployed to the production environment
- An integration testing shall be performed to verify the correctness of the data flows between the MOH systems & a functional testing shall be performed to verify if all functional & non-functional requirements are fulfilled by the integration solution
- The MOH data integration SME (along with the data architect) shall document the test results & the testing process shall be repeated iteratively until the test cases yield the expected results

Integration Solution Deployment:

- The MOH data integration SME shall create a deployment plan before deploying the integration solution into the Production environment
- Once the deployment is complete the deployment details shall be captured in a deployment log
- A round of testing shall be conducted post deployment to verify if the deployment is producing the desired results

Monitoring & Maintenance:

- The MOH data integration SME (along with the data architect) shall monitor the integration solution periodically to identify any defects & document the same in a defect register
- The SME shall make changes to the integration documentations & plan based on the time & complexity required to rectify the defects & also to accommodate any change requests received from end users

Integration Layer Operationalization:

- The MOH data integration SME shall migrate its existing data exchanges between internal & external systems through an integration layer by considering the applicability & business value of each data exchange.

Data Sharing Policy Statements:

1. The Sectorial AI & DMO MUST establish proper data sharing standards and policies to be cascaded and implemented to the rest of the entities.
   1.1. Data sharing requests between entities under the Sectorial AI &DMO MUST follow the standards and policies.
   1.2. Data sharing requests MUST be reviewed, approved, and registered by the entity's own DMO.
2. Permission SHOULD be obtained from the entity DMO before sharing any data that has been shared by the Sectorial AI & DMO with third parties.
3. The entity DMO shall store and process the personal data within Saudi Arabia territory in order to ensure preservation of the digital national sovereignty. These personal data may only be processed outside the Kingdom after the obtaining a written approval from the Regulatory Authority and the Regulatory Authority shall coordinate with NDMO and NCA.
4. Any data sharing request MUST be accompanied by a solid justification or legal basis, unless the data or entities are exempted by a Royal Decree.
5. Data SHOULD only be shared when it delivers a public value and would not inflict harm against national interests, organizations, individuals, or the environment.
6. Data SHOULD always be anonymized (de-identified) from personal identifiers unless it is necessary for the usefulness of the shared data while setting the required controls to protect data privacy in line with NDMO Data Privacy Interim Regulations and the PDPL Regulations.

7. All parties involved in Data Sharing SHOULD make all necessary information available as a part of the integration catalog, this includes but not limited to the required data, purpose behind data sharing request, data sharing mechanism, storage, security controls, and data disposal mechanism.
8. All entities involved in Data Sharing SHOULD have an adequate set of security controls to protect and safeguard data and enable a secure environment for Data Sharing in line with relevant national laws and regulations, and in line with the National Cybersecurity Authority requirements.
9. All entities involved in Data Sharing SHOULD apply ethical practices throughout the Data Sharing process to ensure fairness, integrity, trust, and respect, and go beyond meeting data protection and security standards or other regulatory requirements.
10. The entity SHOULD share data only when all principles are satisfied, and all controls and requirements assigned to the data are met and satisfied.
11. The Sectorial AI & DMO MUST Define and Develop the Roles and Responsibilities for the parties involved in the data sharing process as mandated from the NDMO.
12. All entities involved in Data Sharing SHOULD be held accountable for Data Sharing decisions, for processing it according to the defined purposes while withstand its integrity, and for taking the necessary actions to ensure data quality prior to sharing it, and the implementation of security controls as defined in the Data Sharing agreement and as prescribed by relevant national laws and regulations.
13. Data sharing requests MUST fall into one of two categories currently defined by the Health Sectorial DMO; internal data sharing, which occurs between the internal departments of the entity, and external data sharing, which occurs outside of the entity. The data category MUST be defined for each data sharing request and registered in the integration catalog.
14. **External data sharing request SHALL include but not limited to the following:**
    - **14.1. Receiving the request:**
        - 14.1.1. The Requestor SHALL submit a data sharing request utilizing the approved data sharing form to the entity DMO followed by the signed data sharing agreement.
        - 14.1.2. A Data Sharing Agreement MUST be produced, agreed, signed, and preserved by all external entities prior to any data sharing or exchange, components of the data sharing agreement can be found in the appendix.
    - **14.2. Request assessment & review:**
        - 14.2.1. The DMO MUST review the request form submitted by the external entities, including the requested data and the data sharing agreement.
        - 14.2.2. The DMO officer SHALL check the classification level of requested data prior to any decision or recommendation.
            - 14.2.2.1. If the classification level is not set, the DMO officer MUST classify the data requested as per the Data Classification Policy.
        - 14.2.3. The DMO MUST provide the initial approval for the requested data, or reject it, providing justification.
        - 14.2.4. The Business Unit MUST analyze the request form submitted by the external entities, determine appropriate actions before proceeding with the request or reject it, providing justification supplemented by the DMO recommendation.
        - 14.2.5. The EA SHOULD identify the right architecture for sharing the requested data with the external entities, by ensuring that both parties commit to verifying the security and reliability of the means of sharing used to minimize potential risks, prioritizing secure and trusted data exchange methods, including the Government Service Bus and the National Information Center Network.
        - 14.2.6. Takamul SHALL implement the right architecture based on EA requirements for sharing the requested data with the external entities.

14.2.7. The DMO MUST update the integration catalog to record all the external entities data requests, data sharing agreement, integration channel and the shared data.

14.2.8. If the external entity requires another dataset to be shared, they MUST submit another request.

14.2.8.1. The data sharing agreement SHALL remains the same, the newly requested data will be supplemented in the appendix.

15. Internal data sharing request SHALL include but not limited to the following:

15.1. Receiving the request:

15.1.1. The Requestor SHALL submit a data sharing request utilizing the approved data sharing form the DMO specifying all the data they're requesting.

15.2. Request assessment & review:

15.2.1. The DMO MUST review the request form submitted by the internal entities, including the requested data form.

15.2.2. The DMO officer SHALL check the classification level of requested data prior to any decision or recommendation.

15.2.2.1. If the classification level is not set, the DMO officer MUST classify the data requested as per the Data Classification Policy.

15.2.3. The Business Unit MUST analyze the request form submitted by the internal entities, determine appropriate actions before proceeding with the request, or reject it, providing justification.

15.2.4. The EA SHOULD identify the right architecture for sharing the requested data with the internal entities, by ensuring that both parties commit to verifying the security and reliability of the means of sharing used to minimize potential risks, prioritizing secure and trusted data exchange methods.

15.2.5. Takamul SHALL implement the right architecture based on EA requirements for sharing the requested data with the internal entities.

15.2.6. The DMO MUST update the integration catalog to record all the external entities data requests, data sharing agreement, integration channel and the shared data.

Data Sharing Training and Awareness:

- Data Stewardship Manager shall conduct the Data Sharing training and awareness sessions for all employees involved in the Data Sharing initiatives to ensure that they understand their obligations, responsibilities and the consequences of an unauthorized disclosure or mishandling of data.

Monitoring & Compliance:

The following KPIs shall be considered (but not limited to) by the data integration SME(s) along with data steward and data custodian to monitor periodically compliance to this domain:

- The number of Data Sharing requests received
- The number of Data Sharing requests accepted/denied
- The number of Data Sharing requests raised
- The number of ongoing Data Sharing agreements
- Average duration of Data Sharing requests evaluation process expressed in days
- Data transfer rate between systems / applications
- Latency between data sources and data targets
- Number of SLA violations

Roles & Responsibilities:

The following roles play an important part in governing data integration & interoperability in MOH:

Data Integration SME(s):

- Conduct the initial data integration assessment
- Create the target data integration architecture
- Create the solution design document & integration requirement document for the target data integration solution
- Monitor the data sharing & interoperability KPIs & reporting them to the data governance council
- Develop the data integration solution
- Test & deploy the solution into the production environment
- Monitor the developed solution to identify defects
- Migrate existing MOH data exchanges through the developed integration layer

Data Steward(s):

- Creation of internal & external data sharing agreements
- Provide the data sharing training to employees within their department

Data Custodian(s):

- Assist the data integration SME in creation of data mapping for their respective applications
- Inform data integration SME of any data integration issues identified in their respective applications
- Document details of any data transformations (technical metadata) taking place in their managed systems or applications in the data catalogue

Data Architect(s):

- Assist the data integration SME in creation of the target data integration architecture wherever required
- Review & suggest changes to the integration design document created by the data integration SME

2.10. Data Value Realization Domain

Objective: To establish the requirements for continuous evaluation of MoH data assets for the purpose of identifying data driven use cases that have the potential for revenue generation or cost reduction.

Data Value Realization Plan:

- The DGH and the Head of AI and Advanced Analytics, in collaboration with the Data Owners and Champions shall create a data value realization plan to implement data value realization use cases. The plan shall include, at minimum, the following:
  - Roadmap with the activities and key milestones for the implementation of Data Value Realization Use Cases. The activities shall, at minimum, incorporate what is needed to achieve the specifications in this domain
  - Assignment of the required resources and budget to manage the implementation of Data Value Realization Use Cases.

- The DGH, along with the Data Owners and Champions, shall review the plan periodically & document MOH's progress towards the targets (KPIs) mentioned in the plan.

Data Value Realization Use Cases:

- The Data Owners along with support from Data Champions, shall identify and document Data Value Realization use cases. Further identified use cases shall be reviewed by DGH and approved by the Head of AI and Advanced Analytics.
- The Identified Data Value Realization Use Cases are required, at minimum, to incorporate the two types of Data Value Generation Use Cases as detailed below:
  - **Data Revenue Generation Use Cases**: Data or Data Products utilizable for generating revenue
  - **Cost Saving Use Cases**: Data-driven use cases that shall contribute directly or indirectly to reducing costs

- The Data Owners along with Data Champions shall estimate and document, for each identified Data Revenue Generation or Cost Saving use case, the following:
  - Projected Payback Period for resources invested into implementing the use case
  - Return on Investment (ROI) expected from use case implementation

Pricing Scheme Definition:

- The Data Champions shall determine the pricing for the data/ data product through selecting and documenting the appropriate Pricing Scheme Model (based on the scenarios outlined in the Data Revenue Framework Regulation) for each Data or Data Product MOH intends to utilize for revenue generation and it shall be approved by Data Owner in consultation with DGH and AI and Advanced Analytics Team.
- The Data Owners along with Data Champions shall submit the pricing scheme model recommendation to the relevant committee in MOH that is responsible for data/ data product pricing*

*The specific committee that is responsible for product pricing to be assigned later

Data or Data Product Price Calculation:

- The Data Owners along with Data Champions shall calculate and document the Total Cost for each Data or Data Product MOH intends to utilize for generating revenue for their data domain.
- The Data Owners along with Data Champions shall ensure that the Total Cost of use case(s) development should, at the least, meet the minimum requirement of including the summation of the below values:
    - **Data Collection Cost:** cost incurred during the collection, cleansing, and curating of data/ data products or services
    - **Data Development Cost:** cost incurred during development of analytical models, data visualizations and other value-added services provided on top of collected data/ data products or services

Charging Model Adoption:

- The DGH in collaboration with the Head of AI and Advanced Analytics shall define the appropriate Charging Model for each Data or Data Product MOH intends to utilize for generating revenue or cost reduction.
- Additionally, the Data Owners, in collaboration with the Data Champions, shall document the defined Charging Model. The Charging Model shall be chosen from the following types:
    - **Subscription Model:** a subscription-based model is where a customer pays a recurring price at regular intervals for the service/ product provided
    - **Consumption-Based Model:** a consumption-based model is a service provision and payment scheme in which the customer pays according to the resources used
    - **Freemium / Premium Model:** a premium-based model is where the user is offered free, basic features at no cost, but payments are incurred on the purchase of advanced or additional features for the premium version of the product
    - **One-Time Fee Model:** a one-time fee model is where the customer pays a set price when purchasing the provided service/ product

Data Value Realization Use Cases Monitoring and Maintenance:

The Head of AI and Advanced Analytics in collaboration with the Data Owners and Data Champions shall actively monitor, and maintain the implemented Data Value Realization Use Cases by, at least, performing the following:

- Measuring and validating KPIs (ROI and Payback Period) against the projected values defined in the Data Value Realization Plan
- Developing Change Request documents to accommodate service/ product change requirements from the end-users
- Reporting defects or malfunctions in the implemented use case to the Data Owners and DGH

Data Value Realization KPIs:

The DGH, in collaboration with the Data Owners and Champions shall establish key performance indicators (KPIs) to measure the results of Data Value Realization activities. The KPIs shall, at the least, include the following metrics:

- Number of Data Products developed
- Number of Data or Data Products revenue generation requests raised to MOH
- Number of Data Products that generated revenue

- Total revenue generated from offering Data or Data Products
- Total cost saved from implemented Cost Saving Use Cases
- Data Value Realization Use Case Payback period
- Data Value Realization Use Case Return on Investment (ROI)

Roles & Responsibilities:

Data Governance Head:

- Accountable for MOH's compliance with the Data Value Realization policy. Oversees implementation of the Data Value Realization Plan and reviews progress to ensure achievement of the determined KPIs

Head of AI and Advanced Analytics:

- Develops the data value realization plan, and the identification, development, implementation and monitoring performance of data value realization use cases

Data Owner:

- Provides support and ensures the implementation of the data value realization domain (section 2.10.) including use case identification, ROI and payback period analysis and KPIs setup

Data Champion:

- Provides support for the implementation of the data value realization domain including use case identification, ROI, and payback period analysis and KPIs setup.

2.11. Open Data Domain

Objective: The purpose of this Open Data Policy is to cultivate an environment of trust, transparency, and accountability for health data open to the public, enabling organizations and individuals to make informed decisions. One of the most important factors for the success of a data strategy is the data management and governance program; within this framework, open data stands as a pivotal component due to its role in governance, identification, updating, and dissemination of publicly available data. Such open data initiatives aim to elevate transparency, expedite innovation, and foster growth. Additionally, this policy sets out the requirements and responsibilities of healthcare entities under the jurisdiction of the Sectorial AI and DMO to ensure alignment with relevant Saudi and regulatory standards.

Statements:

- The entity MUST develop a plan and strategy to facilitate the coordination and dissemination of open data. It SHOULD assess the value of each identified open datasets as per its potential applications and benefits, the public interest in the dataset and the data quality of the dataset.
- The datasets shall be prioritized for publication as per the decreasing order of their value.
- The data sets that are classified as 'public' by health entity SHALL be eligible for being identified as open data. In case any datasets are not classified, the entity shall classify them as per the data classification policy.
- Data sets containing detailed data MUST be ensured that they are classified as "Public" to be shared as open data
- All data, other than classified as "Public", MUST be de-identified to make sure that no confidential data gets leaked out if made public and also consider the approach of aggregating the information.
- The entity sharing the datasets MUST be the owner of that dataset. If not, they SHOULD take appropriate permissions from the owner to share the datasets.
- Metadata that defines and explains the raw data should be included with explanations or formulas for how data was derived or calculated to help the user understand the data and avoid misuse of the same.
- Public datasets MUST be as complete and as granular as possible, reflecting what is recorded, in compliance with the data classification policy and data privacy policy (<Link>) (Reference ID: URL).
- The entity SHOULD identify the timeline and frequency of updating and disposing the open datasets based on business requirements.
- Entity MUST assess whether the identified datasets can cause a privacy & security risk to any data subject or to Sectorial AI and DMO before they are published in the open data portal.
- Open datasets SHOULD be made publicly accessible in a machine-readable format that allows automated processing through APIs.
- Data should be shared in a widely used file formats (such as CSV, XLS, JSON, XML) that facilitate machine processing.
- The published datasets SHOULD be updated as per the update frequency specified in the metadata. The update shall be done in the below scenarios:
- There is a change to the data in the dataset.
- There is a change to the underlying metadata in the dataset.
- The entity shall make available the open dataset compiled and aggregated whenever possible to ensure the confidentiality of the data.
- Public datasets SHOULD be available to anyone without discrimination or requirement. Any person

should be able to access open data published at any time without having to identify him/herself or to provide justification for gaining access.

- Public datasets SHOULD be made available to public free of charge.
- The entity SHOULD maintain a registry to record all the open data shared and a version history for its open datasets and document the changes that have been applied to each new version of the dataset.
- Public Datasets SHOULD enable informed civic participation and reinforce governments„ transparency and accountability to improve decision-making and enhance the provision of public services.
- Entities MUST play an active role in promoting the reuse of open data and provide necessary supporting resources and expertise. Entities should actively work on empowering a future generation of open data innovators and engaging individuals, organizations, and the general public in unlocking the value of open data.

Monitoring and Compliance

- All health ecosystem entities are responsible for complying with this Policy.
- The entity should create a compliance monitoring plan that can be used to continually assess the entity`s overall compliance with this policy.
- Key controls should be applied in accordance with the sensitivity of the information. Controls must be physical, procedural, and technical
- Any exceptions to this policy with valid business justification require approval from Sectorial AI and DMO as a certified authority as per law.
- If users are unsure or not clear of any point in this policy, they should seek clarification or advice from Sectorial AI and DMO. at data-office@moh.gov.sa or policy-data-office@moh.gov.sa
- Regulatory Authorities – in coordination with Sectorial AI and DMO – shall develop the mechanisms, procedures, and controls to resolve disputes related to open data policy.
- The Sectorial AI and DMO shall measure and monitor the KPIs related to open data periodically to ascertain entity's progress against the open data plan. The same shall be signed off by the data governance head and published to Sectorial AI and DMO's data governance council and to the regulator.
- The entity shall assess the user response to their published open datasets periodically following the defined open data feedback process to understand which datasets pose greater public demand. The below areas shall be analyzed:
    - No. of user downloads to the dataset.
    - No. of times a dataset has been accessed.
    - Most searched keywords/terms.
    - Most searched data categories.
    - Datasets most requested by users.
- The entity shall re-prioritize the datasets to be published as per the user response to the above metrics as well as the dataset requests received in the open data portal.
- Sectorial AI and DMO shall review the annual reports submitted by entities with regards to their compliance against the policy
- Sectorial AI and DMO is entitled to initiate ad-hoc or periodic compliance audits on any entity and conduct a review of each decision to publish or refuse to publish data.

Roles & Responsibilities:

Entity:

- Create the open data plan
- Identify open datasets in MOH & assessing their value
- Prioritize open datasets for publication
- Acquire open data license from KSA open data portal
- Organize open data awareness campaigns in MOH
- Monitor open data KPIs periodically

Data Privacy & Protection Manager:

- Assess identified open datasets for any personal data protection risks

Data Stewards:

- Rectify data quality gaps of open datasets
- Update metadata, data provenance & version history against the open datasets

Data Custodians:

- Publish identified open datasets & their APIs in MOH's open data portal
- Convert open datasets into various identified formats for publication

Data Owner:

- Providing approval for the publication of the open datasets

2.12. Freedom of Information Domain

Objective:

The purpose of the policy is to promote transparency, accountability, and public access to healthcare information. It also fosters an open and accountable government by establishing procedures for Individuals to request and obtain information from healthcare entities. Within the overarching structure of our data governance program, this policy stands as a central pillar, emphasizing the critical importance of receiving, analyzing and strategic dissemination of data made available to the individuals. The aim is to significantly enhance transparency, catalyze innovation, and drive sustainable growth, while ensuring strict adherence to the highest standards of data integrity and privacy. Additionally, this policy sets out the requirements and responsibilities of healthcare entities under the jurisdiction of the Sectorial AI and DMO to ensure alignment with relevant Saudi and regulatory standards.

Statements:

- The entity shall prepare and document the necessary procedures to manage, process, and document the fulfilled requests, denied & time to fulfill the request. It shall also define the roles and responsibilities of the concerned staff and shall decide on the cases to be notified to the Sectorial AI and DMO as per the administrative hierarchy and in accordance with the time specified for processing requests.
- The entity SHALL be responsible for preparing and implementing policies and procedures related to exercising the right to access or obtain public information, and the entity's head is responsible for approving and adopting it.
- Entities MUST enable the process of requesting the information through necessary platforms or through templates.
- The entity SHALL verify the identity of individuals before granting them the right to access or obtain information in accordance with the controls determined.
- The entity SHALL only provide information to the requestor for those data sets for which they are the rightful owner.
- The entity shall provide options to enable the disclosure of confidential or secret information through internal platforms, such as a data lab or secure systems, for sharing such information with requestors.
- The entity MUST ensure the requested information complies with the relevant policies such as Data Classification, Open Data etc. that are defined by the Sectorial AI & DMO Office. (Reference ID: URL)
- Individuals SHOULD have the right to access information related to healthcare entities, activities to enhance integrity, transparency, and accountability unless it falls under below categories:
    - Information that, if disclosed, may harm the Kingdom’s national security, policies, interests, or rights.
    - Information that, if disclosed, may result in the disclosure of personal health information, including patient identities, medical records, or other details.
    - Health-related documents and information obtained in agreement with another state, international healthcare organizations, or entities, classified as protected due to their sensitive nature.
    - Information related to inquiries, investigations, checks, inspections, and monitoring in respect of healthcare fraud, malpractice, or ethical violations.
    - Commercial, industrial, financial, or economic information specific to healthcare, including

pharmaceutical pricing and hospital financial data, that, if disclosed, may result in unfair market advantages or losses.
    - Information related to scientific research or technological advancements in healthcare, including details of ongoing clinical trials or unpublished research, which may infringe on intellectual property rights if disclosed.
    - Information and the like, which are protected, confidential or personal under another law, or require certain legal action to be accessed or obtained.
- The entity SHOULD mention any restrictions to the individual, requesting access or trying to obtain protected information in a clear and explicit manner.
- The entity SHALL manage and record requests to access public Information, including requests that are rejected or require extension.
- The entity MUST determine and provide possible means (forms for requesting public information) – whether paper or electronic – through which the applicant can request access to public information.
- The entity SHOULD set the necessary standards for determining the fees if any for processing requests to access or obtain public information based on the nature of the data, its size, the effort spent, and the time taken.
- The entity SHALL document all records of requests to access or obtain public information and the decisions taken on these requests, provided that these records would be reviewed to address cases of misuse or non-response.
- Individuals SHOULD be able to file a notice of appeal against the decision to refuse the request for access to information.
- The entity MUST notify the requestor – in an appropriate manner – if his request is rejected in whole or in part, explaining the reasons for denial and highlighting the right to appeal and how to exercise this right within a period.
- The entity SHOULD launch awareness-raising programs to promote a culture of transparency and raise awareness pursuant to the Freedom of Information Policies and Procedures approved by the senior management of the entity.
- The entity SHALL be responsible for monitoring compliance with the Freedom of Information Policies and Procedures on a periodical basis and for presenting the results to the head of the entity (or his designee). It shall also determine and document the corrective measures to be taken in case of non-compliance and shall notify the Sectorial AI and DMO as per the administrative hierarchy.

Roles and Responsibilities:

Data Governance Head (DGH):

- The DGH will lead and oversee the achievement of the freedom of information agenda at the health entities level.

DG Policies and Procedures Manager:

- Prepare, manage and maintain the Freedom of Information policies, processes and procedures, including approving and adopting it with the help of Entity officer

Open Data and Information Access Officer:

- Supervise the processing of requests for access to public information in accordance with freedom of information laws and regulations
- Document records of freedom of information requests and ensuring publication required information
- Provide responses to requests for information, including all refusal notices, having liaised with colleagues, reviewed information held and considered any public interest arguments or exemptions
- Maintain the systems and processes used to log and record requests for information received under Data Protection and Freedom of Information legislation.

2.13. Data Classification Domain

Objective:

The purpose of this policy is to adhere to the national mandate laid out to classify existing and newly generated health data using a defined data classification template that will enable the ecosystem to apply the right business, technical, and security controls to identify, protect, and better utilize healthcare data for the purposes of data sharing, processing, storage, and access and help the entities to comply with the regulations. This policy also outlines the requirements and responsibilities of healthcare entities working under the jurisdiction of Sectorial AI and DMO classification and ensures that the applicable and relevant security controls are set in place to reduce the risk of data breaches and security incidents facilitating the protection of health information assets in line with national and international regulatory requirements.

Statements:

- The entity's internal stakeholders SHOULD collaborate and create a data classification plan to manage and orchestrate data classification activities. The plan should be periodically reviewed and updated based on the need.
- Prior to classifying the datasets, the entity MUST formulate a classification prioritization list, ranking all the datasets in order of their classification priority.
- The entity SHOULD identify and make a complete list of all existing data assets, including both electronic and paper-based formats.
- The entity MUST align with the controls defined by NCA based on the data classification level.
- When handling data, all users MUST do so in accordance with and be responsible for adherence to the AI & DMO data classification policy. Periodic auditing of adherence to this policy is the responsibility of the sectorial health AI & DMO.
- The data MUST be classified into below categories: Further details available in Annexure A
    - Top Secret
    - Secret
    - Confidential
    - Public
- Users MUST ensure that data is appropriately labeled in accordance with the health data classification policy and any bespoke requirements as required by the wider health sector.
- Data impact assessment (Refer to Annexure B) MUST be performed on the hosted datasets owned by the entities based on the framework designed (<link>) (Reference ID: URL)

- Data specific to healthcare MUST be classified as CONFIDENTIAL by default unless its nature or sensitivity requires a lower level of classification and protection; or is classified as public.
- Data MUST be classified upon creation or upon being received from another entity and the classification exercise should be timebound.
- If the information includes an integrated set of data with different classification levels, the highest classification level MUST be applied to the aggregated data.
- Data sharing and transfer SHOULD be done based on the classification and data sharing policies laid out by sectorial AI and DMO.
- When there is a change in the classification of data or information by the health ecosystem, that change MUST be documented with the reason for the reclassification. (<link>) (Reference ID: URL)
- Re-classification of data MUST be done if the classification duration expires, or the original level of protection is not needed for the data or if the data is wrongly classified. In case of any change in the classification, it SHOULD be documented with the reason for the reclassification. (<link>) (Reference ID: URL)
- The entity shall establish and cement key performance indicators (KPIs) to measure the progress on the implementation of the data classification plan.

Data Classification KPIs:

- The Data Owners, in collaboration with Data Stewards shall establish and cement key performance indicators (KPIs) to measure the progress on the implementation of the data classification plan. The KPIs shall, at the least, include the following metrics:
    - % of datasets and artefacts classified
    - % of datasets and artefacts classified by Data Classification Category
    - % of 'Low' impact data classified as 'Confidential'
    - % of classified datasets and artefacts that have been reviewed and approved by each Data Owner
    - % of classified datasets and artefacts that have been reviewed and approved by each Data Owner and DGH
- The DG Compliance Manager shall track and monitor the established Data Classification KPIs and report/ escalate the required remedial tasks or activities as needed to the DGH so that the Data Classification Plan is kept on track.

Data Register:

- The DGH shall establish a data register that can host, maintain, and generate reports on performed data classification activities, along with key information such as the list of identified data assets, impact level and the classification category assigned to all identified data assets

- The Data Custodians shall capture the results of data classification activities, along with key information such as the list of identified data assets, impact level and the classification category assigned to all identified data assets within the data register

Roles & Responsibilities:

Chief Data Officer:

- Accountable for Entity compliance to the data classification domain. Reviews the completed data classification exercise to ensure overall validity of the assigned classification categories to MOH's datasets and artefacts.

Data Governance Head:

- Responsible for Entity compliance to the policy. Oversees and coordinates overall implementation of the Data Classification Plan and reviews progress to ensure achievement of the determined KPIs.

Data Owner:

- Review and approve the classification category determined by the data stewards as well as inputs given on other data classification activities (such as identification). Responsible for development of the appropriate data classification KPIs.

Data Champion:

- Providing support for data classification plan development, classification prioritization list and data identification.

Data Steward:

- Conducting the impact assessment and assigns the appropriate classification category for datasets and artefacts within their domain. Gives their input on other data classification activities (such as identification).

Data Custodian:

- Responsible for capturing data classification activities within the data register, capturing the impact level and classification category within the data catalog tool/ solution, and documenting the complete list of the Data Identification results for all data assets within their data domain.

Annexure A

Classification	Impact Level	Definition
Top Secret	High	Data shall be classified as "Top Secret", if unauthorized access to or disclosure of such data or its content adversely and exceptionally affects in a way that is difficult to resolve: • National interest including violations of conventions and treaties, adverse damage to the reputation of the country, diplomatic relations and political affiliations, operational efficiency of the security or intelligence operations of military forces, national economy, national infrastructure, and Government functions, and/or • Organizations functionality causing damage to the national interest, and/or • Individuals' health and safety at a massive scale and privacy of Protected Individual personnel, and/or

			• Catastrophic damage to the environment or natural resources
	Secret	Medium	Data shall be classified as "Secret", if unauthorized access to or disclosure of such data or its content adversely affects: • Affects national interest such as damage to the reputation of the country, diplomatic relations, operational efficiency of the security or intelligence operations of military forces, national economy, national infrastructure, Government functions. • Financial loss of KSA organizations that leads to bankruptcy or inability of the organizations to perform their duties or major loss of competitive abilities or combination thereof, and/or • Causes significant harm or injury impacting life of individuals. • Causes long-term damage to the environment or natural resources. • The investigation of major cases such as terrorism funding.
	Confidential	Low	Data shall be classified as "Confidential" data if unauthorized access to or disclosure of such data or its content causes: • Contained negative effect on government entities' operations, KSA economy, or negative effect on individuals' interests. • Damage to any entity's assets and limited loss to its financial and competitive status, and/or • Contained damage in the short-term to the environment or natural resources.
	Public	Low, None	Data shall be classified as "Public", if unauthorized access to or disclosure of such data or its content has no impact on: • National Interest, • Organizations, • Individuals, or • Environment

Annexure B

	Top Secret	Secret	Confidential	Public

Considerations	Level of Impact			
	High	Medium	Low	None
Would the information be subject to international or national media interest? Would it give negative publicity?	Reputation is adversely affected	Reputation is affected to some extent	Reputation is not affected	No impact on the National Interest
Would the information drain or pose any risk to the relationship with friendly countries? Would it raise international tension? Could it lead to protests or sanctions from other countries?	Diplomatic relationships and political affiliations are broken, and/or conventions and treaty terms are compromised	Diplomatic relationships are compromised and will be negatively affected in the long term	No effect on the Diplomatic relationships or very minimal effect in the short-term	
Would this information if released help with the identification or conduct of terrorist or serious crimes? Would it create an alarm to the public?	The operational efficiency of the security or intelligence operations of military forces is significantly affected and compromised	The long-term effect on the ability and efficiency of the security and military forces to investigate or prosecute serious organized crimes causing internal operational instability	Impeding the detection of small crimes in the short term with no to minimal effect in regional police operational stability	
Would this information if disclosed cause losses to the overall KSA economy?	The long-term effect on KSA economy with an unrecoverable decrease in the GDP, stock market rates, employment rate, purchasing power, and/or other relevant indicators. All the country sectors are affected	The long-term effect on the KSA economy with a recoverable decrease in the GDP, employment rate, stock market rates, and/or purchasing power. One or more sector(s) are affected	Minimal or no effect on the KSA economy with a quick recoverable decrease in the GDP, employment rate, stock market rates, and/or purchasing power. Not more than one sector is affected	
Would unrestricted access to such information cause any interruption of the critical assets of the country (i.e., Energy, Transport, Health…)? In case of a cyber-attack would the critical services of the country still be available?	Failure and long interruption of critical national infrastructure assets security and operations – Several sectors are affected, and normal life is interrupted	Failure and short interruption of critical national infrastructure assets security and operations – One or more sectors are affected	No effect or short-term effect on local/regional infrastructure assets security and operations	

Would the inadequate release of the information have the potential to limit the availability of the Government to carry out daily operations and business functions?	All Government entities are impaired to conduct their functions and daily operations for a long period of time	One or more Government entities are not capable of delivering one or more of their functions for a short period of time	One or more Government entity non-core function(s) are compromised for a short period of time	
Would disclosure of this information lead to third parties,, financial loss or bankruptcy? For example, consider the possibility of fraud, illegal transfers of funds, illegal appropriation of assets	High impact on the KSA organizations to the extent it causes damage to the national interest	Organizations incurring heavy financial loss that could lead to bankruptcy	Limited damage to entity assets with limited financial loss	No impact on the Organizations
Would the release of this information cause any damage to private organizations in the country? Could it mean the loss of its leading role or of any of its assets? Would it lead to a significant number of employees being fired? Would it affect the competitiveness of the organization?		The entity cannot perform any of its functions; severe loss of competitiveness	The entity cannot perform one of its key functions or the organization's effectiveness has been reduced; Limited loss of competitiveness	
Would the access to this information mean the release of names or locations etc.? (e.g., name and location of undercover agents, people under protection orders)	General or massive loss of life; Loss of life of an individual or group	Significant harm or life injury impacting the life of an individual	Minor injury with no risk to the life or health of the individual	No impact on the Individuals
Would compromise of this information violate the Data Privacy Regulation? Would it infringe any Intellectual Property Rights?	Personal information of a VIP person has been disclosed affecting national interest	Personal information of a VIP person has been disclosed	The personal information of an individual has been disclosed	
Would this information be used to develop any service/product that could potentially destroy the environmental or natural resources of the country?	Irrecuperable and catastrophic effects on the environment	Long-term damage to the environment	Short-term and limited damage to the environment	No Impact on the Environment

2.14. Personal Data Protection Domain

Objective:

The Data Privacy & Protection domain defines MoH (herein referred to as MOH or 'ministry' or 'Organization') position on data privacy & protection for personal data collected, used, processed, stored, accessed, shared internally, and shared externally with 3rd parties by the ministry.

The domain sets out a direction on the following personal data protection principles:

- Lawfulness, Fairness & Transparency
- Purpose Limitation
- Data Minimization
- Accuracy
- Storage Limitation
- Integrity & Confidentiality
- Accountability

Personal data protection plan:

- The data privacy & protection manager shall create a personal data protection plan for addressing the strategic & operational requirements for data privacy.

Personal data protection assessment:

- The data privacy & protection manager shall conduct an initial personal data protection assessment (PIA) & also on a periodic basis by leveraging the defined privacy impact assessment process & the personal data protection initial assessment guideline to understand the current maturity of personal data protection in MOH & identify potential risks.
- In addition to the yearly assessment, a PIA shall also be conducted by leveraging the defined privacy impact assessment guideline in the below scenarios:
- There is a new processing activity taking place that involves personal data or involves profiling/ behavioural monitoring of data subjects
- There is a change in the nature, scope, or purpose of any processing activity involving personal data
- The Data Privacy & Protection manager shall be responsible for overseeing mitigation of the risks identified in the DPIA.
- The data privacy & protection manager shall store records of all the identified personal data elements & processing activities (along with their metadata) in a personal data protection register.

Personal Data Inventory:

- The data privacy & protection manager shall maintain a central inventory of all personal data elements that are collected & processed by MOH's various business functions
- The required details shall be captured against each personal data element as mentioned in the personal data protection controls

Privacy Notice Management:

- MOH shall provide a privacy notice to data subjects before obtaining their consent for the collection & processing of their personal data.

- The notice shall be verified & approved by the data stewards before it is presented to the data subject

Privacy Consent Management:

- MOH shall collect & record the consent of data subjects before collecting or processing their personal data. The consent collection & modification process shall be automated as much as possible
- MOH shall record parental consent before collecting & processing personal data of children (below 18 years of age)
- The records of consent shall be stored in a consent repository to ensure an effective audit trail

Consent Modification:

- The data stewards shall communicate details of any consent modification to respective data custodians for reflecting the changes in their relevant applications.
- For consent expiry, Data stewards shall decide if consent renewal from data subjects is required.
- For any business process change, the data steward shall decide whether consent renewal is required & inform the Data Privacy & Protection manager regarding any changes required to MOH's privacy policy.

Preference Centre Provisioning:

- MOH shall provision a preference centre for data subjects to modify their consent. The data privacy & protection manager shall be responsible for managing & updating the preference centre.

Personal data processing:

- MOH shall adhere to the below principles while processing personal data:
    - Lawfulness & transparency
    - Purpose limitation
    - Storage limitation
    - Data minimization
    - Accuracy
    - Accountability
    - Integrity & confidentiality

Please refer to definitions for a brief description of each of the above principles

- The data stewards of each department shall be responsible for ensuring compliance to each of the above principles
- To demonstrate transparency & accountability, MOH shall store records of all its processing activities (ROPA) in a personal data protection register
- MOH shall verify the personal data provided by data subjects at the time of collecting personal data & remove any unnecessary data collected before it is stored in MOH systems
- MOH shall verify the quality of the personal data at the time of its collection & also at regular intervals to ensure that it is complete, accurate & up to date

- MOH shall implement appropriate technical & organization measures (e.g. encryption, anonymization, de-identification, access control, firewalls) to maintain the security of the processed personal data.
- MOH shall erase or anonymize any personal data collected once it has fulfilled its processing purpose or arrived at the end of its retention period
- MOH shall ensure that personal data is protected in all MOH implementation projects by following the defined privacy by design guideline

Data Subject Rights:

- MOH shall cater to the below data subject requests while processing their personal data:
    - **Right to be informed:** MOH shall inform data subjects of the legal basis and the purpose for the collection & processing of their personal data
    - **Right to Access:** MOH shall ensure that data subjects can obtain a copy of their personal data in possession with MOH when requested. MOH shall also provide confirmation (if requested) to data subjects on whether their personal data is being processed, the categories of personal data processed, the processing purpose, the recipients of the data & the storage & retention period of the personal data
    - **Right to Rectification:** MOH shall facilitate data subjects to rectify, complete or update their personal data that is processed by MOH, without undue delay.
    - **Right to Erasure:** MOH shall facilitate data subjects to erase their personal data from its systems in case the data has already fulfilled its processing purpose, the processing has been unlawful, or the data subject has withdrawn consent.
    - **Right to Restrict Processing:** MOH shall restrict or suppress the processing of the personal data of data subjects when requested (in case they feel that the processing is unlawful, their rights are being overridden by MOH's interests, the data processed is inaccurate or the data has fulfilled its processing purpose).
    - **Right to Portability:** When requested by the data subjects, MOH shall provide them their personal data in a structured, commonly used and machine-readable format. MOH shall also directly transmit this information in above format to other third-party organizations requested by the data subject.
    - **Right to object:** MOH shall stop the processing of personal data or stop using it for direct marketing purposes when requested. MOH would need to cater to this request unless it has legitimate grounds for such processing.
    - **Addressing the data subject requests:**
    - MOH shall verify the identity of the data subject prior to responding to their requests
    - The process of catering to data subject requests shall be automated
    - The data stewards (& the data stewardship manager, where applicable) shall be responsible for addressing the data subject requests
    - For Right to Erasure/Rectification, the data stewards shall collaborate with the respective data custodians to erase/rectify the data from MOH systems
    - Timeline for responding:
    - The data steward shall respond to the data subject request within one month.
    - In case more time is required, the reasons for the delay shall be communicated to the data subject & one additional month can be taken to respond.

Personal data breach notification:

- The data privacy & protection manager shall assess the level of risk towards affected data subjects in case of a personal data breach & leverage the defined personal data breach management process.
- The data privacy & protection manager shall notify regulatory authorities & affected data subjects within 72 hours in case of a significant data breach, & also update them periodically on the breach status & remedial actions taken.
- The data privacy & protection manager shall be responsible for documenting the details of the breach & the corresponding remedial actions taken in a personal data breach register
- The Information Security Department shall implement required remedial actions to control the breach & restore any data deleted, stolen, lost or damaged during the personal data breach back to its original location

Vendor Risk management:

- MOH needs to execute Data Processing Agreement with third parties (data controllers & data processors) for the following cases:
    - The third party collects, processes, uses, stores, analyses, retains personal data on MOH's behalf
    - MOH shares personal data with 3rd parties for processing, storage, analysis, and retention for any business process
- The data privacy & protection manager, along with the data stewards shall conduct periodic privacy assessments of MOH's third-party vendors.
- Any gaps identified during the assessment needs to be notified to the data privacy & protection manager
- The data privacy & protection manager would collaborate with the third party to ensure the gaps are remediated

Data privacy compliance monitoring & audit:

- Risk Monitoring: MOH's data stewards shall ensure that their respective departments comply with MOH's Personal data protection domain (section 2.14.). They shall monitor the status of the data privacy risks identified during Personal Data Protection Assessments periodically to ensure their resolution.
- Compliance Reporting: The data privacy & protection manager shall monitor the KPIs periodically to ensure effective performance of the data privacy program. The KPIs reported shall be documented and signed off by the data governance head and also shared during meetings with the steering committee and data governance council.

Data Privacy artefacts:

- For building a comprehensive data privacy program, the following list of documents need to be created by MOH as per the defined controls:

- **Personal Data Repository**- The document aims to provide details of all personal data elements processed by MOH
- **Personal Data Protection Register**-The document aims to provide details of all personal data processing operations carried out by MOH
- **Personal Data Protection Policy (Inc. data retention domain)-** The document provides details of how MOH processes personal data, data security controls used and data subject rights
- **Privacy Notice-**The document mentions the various purposes for which the personal data is being collected from the data subject
- **Data Subject Consent Form-**The document provides an audit trail of the consent, e.g. the consent collection timestamp, data subject details and purposes consented to by them
- **Supplier Data Processing Agreement-**The document provides details of safeguards to be incorporated by third party vendors of MOH
- **DPIA Register-**The document covers details of all DPIAs carried out by MOH in the past 2 years
- **Data Breach Register-**The document provides details of all personal data breaches in MOH in the past 2 years
- **Data Breach Notification form-**The document provides details of the personal data breach for regulatory reporting

Personal Data Security:

- MOH shall follow the PDPL personal data protection guidelines to ensure the safety and security of processed personal data
- MOH shall only allow authorized users to view, update, export, download or delete personal or sensitive personal data. The defined data access request process can be followed for providing access to a new user or modifying access privileges of existing users
- MOH shall process personal data only within the KSA territory and obtain a written approval from NDMO before processing personal data outside the KSA territory
- MOH shall remove or disable user accounts of resigned, deceased or transferred employees immediately.
- The information security department delete or anonymize personal data once it has fulfilled its processing purpose
- The information security manager shall maintain access logs for MOH systems that store or process personal data
- The information security manager shall periodically review the access privileges provided to users for systems that contain personal data to prevent any unauthorized access to the data. The access privileges shall also be reviewed upon change of responsibilities or employee status for the relevant authorized user

Personal data protection training:

- The data privacy and protection manager along with data stewards shall conduct a personal data protection training for the employees of each department.

- The data privacy and protection manager shall decide on the frequency of the training & the data steward shall decide the attendees for the same within their department.

Roles & Responsibilities:

Data Privacy & Protection Manager:

- Create a personal data protection plan
- Conduct personal data protection initial assessment
- Assess risks based on PIA responses
- Oversee mitigation of personal data risks identified during PIAs
- Notify regulator & data subjects in cases of personal data breach
- Create MOH privacy policy
- Monitor & report personal data protection KPIs
- Create a list of personal data elements & categorizing them
- Create & Maintaining Records of processing activities
- Create & Maintaining purpose repository
- Document personal data breach details in breach register
- Create & Maintain the personal data protection register
- Create supplier processing agreement templates & employee confidentiality agreement templates
- Manage the consent preference centre
- Conduct ad-hoc PIAs
- Perform vendor risk assessments
- Conduct training programs for personal data protection

Data Stewards:

- Monitor day-to-day compliance to personal data protection domain & processes
- Review privacy notices to be provided to data subjects
- Communicate any consent modification to data custodians
- Handle data subject requests

Data Custodians:

- Make changes to personal data processes in their applications based on data subject consent provided
- Update or erasing personal data in their applications to cater to right to erasure/rectification requests

Information Security Department:

- Implement data security controls for protection of personal data as per defined ISD personal data protection guidelines
- Verify data subject identity for submitted requests

3. References

- SDAIA Regulatory Arrangements عنوان رئيسي للمستند (sdaia.gov.sa)
- Policies & Regulations Data Standards Document (sdaia.gov.sa)
- Data classification Policy Microsoft Word - 2 - السياسات -EN - NA .docx (sdaia.gov.sa)
- Personal Data Protection Law https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf
- Data Sharing Policy Microsoft Word - 2 - السياسات -EN - NA .docx (sdaia.gov.sa)
- Freedom of Information Policy Microsoft Word - 2 - السياسات -EN - NA .docx (sdaia.gov.sa)
- Open Data Policy Microsoft Word - 2 - السياسات -EN - NA .docx (sdaia.gov.sa)