UNITED ARAB EMIRATES
MINISTRY OF HEALTH & PREVENTION

MOHAP : ENTERPRISE DATA MANAGEMENT FRAMEWORK

STATISTICS & RESEARCH CENTER

Document Control

Document information

	Document Author	Reviewed By	Approved By
Job Title	Varunendra Verma	Dr. Shaikha Abdool	Dr. Alya Harbi
Signature			
Date			

Revision History

Issue No.	Issue Date	Changes Description	Author	Approved By
01	09/05/2022	Version 1	Binu George	Dr. Shaikha Abdool
02	05/09/2022	Version 2	Varunendra Verma	Dr. Shaikha Abdool
03	13/12/2022	Version 3	Varunendra Verma	Dr. Alya Harbi
04	30/1/2026	Version 4	Varunendra Verma	Dr. Shaikha Abdool

ABBREVIATIONS AND ACRONYMS

Abbreviation	Full Form
AJCC	American Joint Committee on Cancer
C.R.U.D	Create, Read, Update and Delete
CDE	Critical Data Elements
CIA	Confidentiality, Integrity and Availability
DHA	Dubai Health Authority
DOH	Department of Health – Abu Dhabi
DQ	Data Quality
DQMS	Data Quality Management System
ETL	Extract, Transform and Load
HIS	Health Information Systems
ICD	International Statistical Classification of Diseases and Related Health Problems.
ICT	Information Communication Technology
ILO	International Labor Organization
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
MOHAP	Ministry of Health & Prevention
SRC	Statistical & Research Center
SEER	Surveillance, Epidemiology and End Results Program
SLA	Service Level Agreement
SOA	Statement of Applicability
SQL	Structured Query Language
WHO	World Health Organization

FOREWORD

The **Statistics and Research Centre (SRC)** of the **Ministry of Health & Prevention (MOHAP)** have prepared this **Enterprise Data Governance** document which essentially describes the implementation of Data Governance across all the constituent departments of the MOHAP.

This document contains information about the below aspects pertinent to Data Governance;

- Current Data Architecture in MOHAP
- Key Roles & Responsibilities across the organization
- Data Governance : Framework , Ownership and Policies
- Data Quality : Dimension, Management Process, General Issues & Activities to overcome the issues, Metadata management
- Data Security & Protection : Key CIA Aspects, Protocols, Laws, Policies and Data Confidentiality
- ISO Certifications achieved by MOHAP related to Data Security and Data Quality

The rationale behind presenting this document is for obtaining a holistic view of the enterprise level Data Governance structure in MOHAP. Since there exists a copious amounts of UAE Citizens' Healthcare Data that is scattered across numerous departments and facilities in MOHAP , It is imperative to have a central structure in place that will govern the way data is collected, processed, stored and shared with utmost quality, efficiency and security.

As a central Data Governance body of MOHAP, It is our department's endeavor to ensure successful implementation and continuous improvement of the defined framework and activities mentioned in the document. We appreciate the support and co-operation of all our fellow MOHAP departments in embracing all the concepts and existing structures described here to help us collectively achieve the ultimate goal of secure and robust data management.

TABLE OF CONTENTS

1. LIST OF FIGURES

2. LIST OF TABLES

3. INTRODUCTION

3.1 Executive Summary

Data Governance is the need to effectively manage and integrate vast and often disparate volumes of business data in order to be able to extract competitive information in a timely manner. The governance enabler is the means by which a healthcare entity provides data analytics capability and stewardship. The MOHAP has a comprehensive Enterprise-Wide Data Governance Framework which serves to govern the vast and rich amounts of diverse data present across the numerous departments of the ministry. Each of the departments abide by the Data Governance and Management framework as defined in this document.

3.2 Purpose

The purpose of this document is to provide an overview of the entire Data Governance processes currently present in MOHAP. These standards are intended to break down data silos across the multiple departments within MOHAP thereby fostering a centralized data architecture and harmonization of the data through a collaborative process with internal and external stakeholders.

3.3 MOHAP Overview

MOHAP is the federal healthcare regulatory authority in the United Arab Emirates. It introduces, updates, and implements healthcare policies that are followed across all the clinical facilities in the country. It aims to promote the health of the community through the provision of comprehensive and innovative health services in fair and global standards and to play the regulatory and supervisory role in the health sector through sophisticated and integrated health legislative system. Below are the Mission and Vision of the organization.

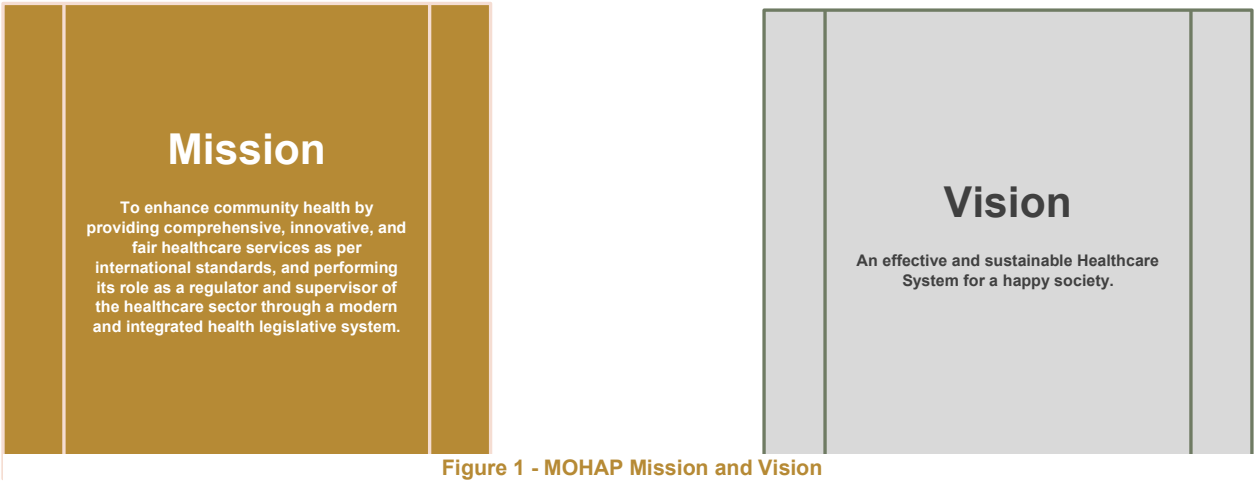


Figure 1 - MOHAP Mission and Vision

4. DATA ARCHITECHTURE (CURRENT SITUATION)

4.1 Overview

The below diagram demonstrates the current Data Architecture in MOHAP encompassing the interconnected department-wise Data Systems, Activities performed on data acquired from these systems and ultimate use of the final data.

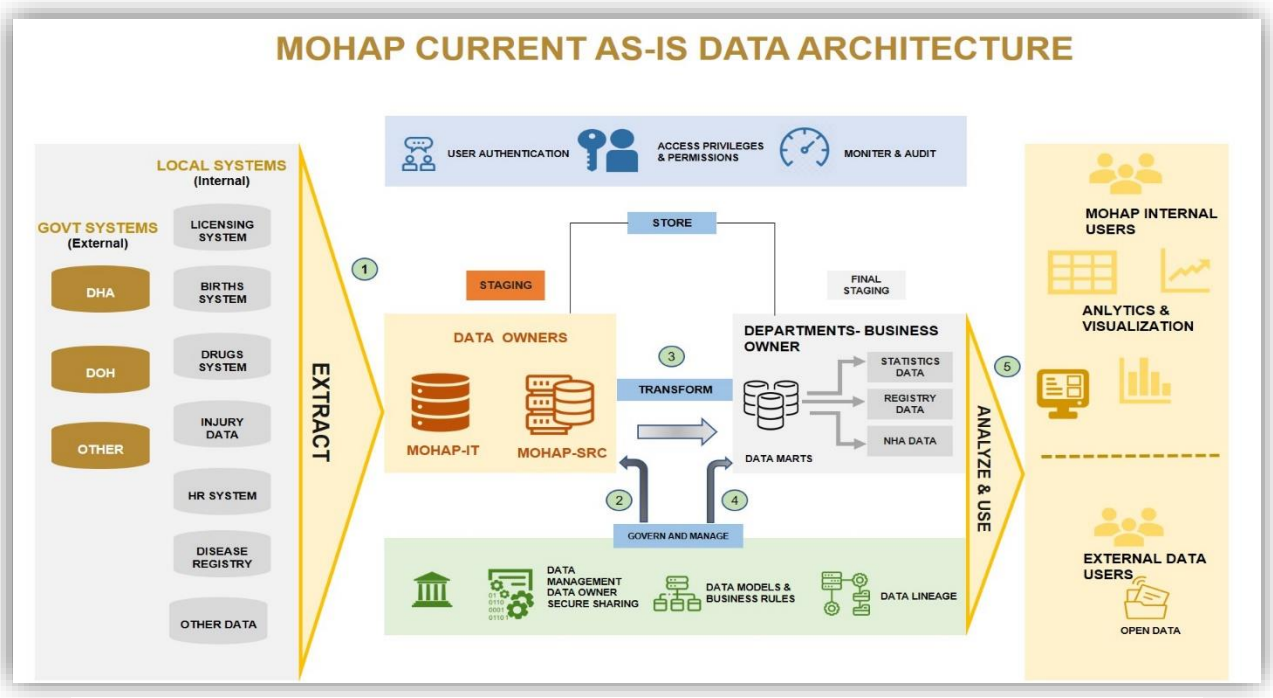


Figure 2 - MOHAP Data Architecture (AS-IS)

Stage 1

Data from various Systems internal and external to MOHAP are extracted and stored in designated system-specific Databases which are governed entirely by MOHAP-IT department. However the ultimate **Data Ownership** of these data sets lies with the MOHAP - Statistical and Research Center (SRC) department. This is considered as the **STAGING** area of the system-wise data in databases.

Stage 2

The databases present in the MOHAP-IT ecosystem are governed by experienced Database Administrators who undertake data management protocols related to secure storage & sharing, data protection and availability, back-up and recovery, database tuning etc. Additionally, The MOHAP-IT Security and Quality team ensure that officially **documented** Data Security & Quality Policies are actually implemented.

Stage 3

Thereafter if any MOHAP-Department needs the data from these databases, then their officially appointed Business Owners either directly extract data from the system or the IT team extracts and shares the data (in the form of raw data or report excels file) with them. This data is then securely stationed in the official Shared-Folder servers created by MOHAP-IT. This is considered as the **FINAL STAGING** area of the system-wise data in databases.

Stage 4

Similar to Stage 2, the data on the department-specific shared-folder servers is severely scrutinized. Designated Data Analysts and Business Owners perform elaborate set of Data Quality Measures (Highlighted in section 7.5-Activities) to ensure the final data present with each department is accurate , conforming to requirements , clean and ready to be disseminated.

Stage 5

The final subject-specific data across clinical, statistical and operational areas present with each department is then utilized for research, analytics, dashboarding, Key Indicator calculations , reporting and various other purposes.
Centrally, MOHAP - Statistical and Research Center (SRC) department is responsible for the UAE-LEVEL data dissemination of the aforementioned final data with both internal and external entities (public and private institutions).

For reference, Comprehensive list of Data Systems in MOHAP along with their Department Owner and corresponding Business Owner, Data Usage and Integration network (internal and external) are present in the Appendix section - 9.7 MOHAP Application Topology.

5. ROLES AND RESPONSIBILITIES

5.1 Overview

There are a myriad of roles in an organization having specific data-oriented tasks that are required to be undertaken, however the most cardinal viewpoint that ensures an effective and successful implementation of enterprise-wide Data Governance is stated below;

SUPPORTING DATA GOVERNANCE IS THE RESPONSBILITY OF EVERY ORGANIZATIONAL ROLE

5.2 Role Definitions

Below mentioned are the key Data Governance roles functioning in MOHAP along with their well-defined responsibilities and example of key MOHAP Positions that essay these roles.

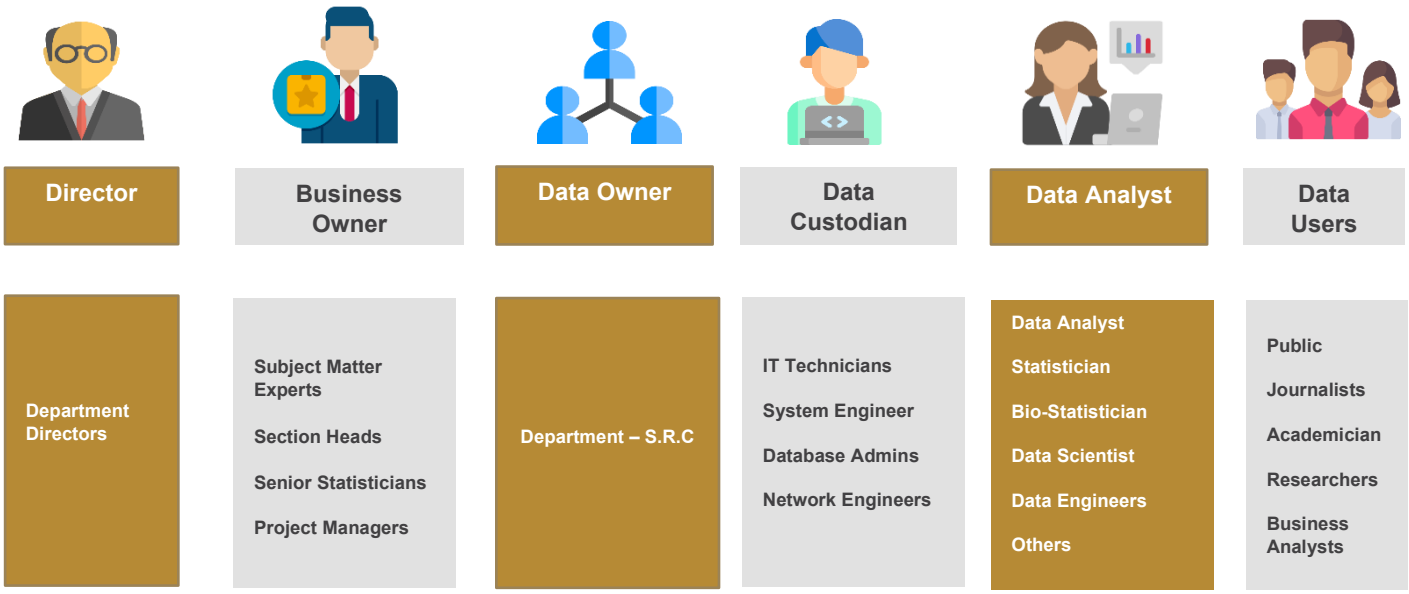


Figure 3 - Data Governance - Roles & Responsibilities

Role	Description	Responsibilities
Director	Management personnel who is chiefly responsible for all Business related decisions and actions that impact the underlying data generated within their unit. Ex: Directors of each MOHAP department	• Managing Data goals of the enterprise. • Leading development of policies , standards , processes and procedures to ensure the continuous improvement in data quality.

Business Owner	Individual that has direct operational responsibility within each business unit for the management of one or more type of data Ex: Section Heads of each MOHAP department	• Governance and Ownership of key Data Systems belonging to his/her department. • Review and Approval of data requests pertaining to data belonging to the key Data Systems. • Finalize requirements, resolve queries and address concerns pertaining to the data belonging to the key Data systems.
Data Owner	Department which has central responsibility for Data Governance. Ex: Statistics and Research Center	• Accountability for all aspects of data governance and quality in Business Unit. • Review and Approval of sensitive or classified data prior to sharing with requestors. • Defining the usage and accepted terms of Critical Data Elements (CDEs) published in a data dictionary. • Identifying , resolving and escalating high priority/impact data quality issues. • Providing overall data management strategy, ongoing sponsorship, leadership, active engagement, and incentives within their Business Unit.
Data Custodian	Individual responsible for the operation and management of systems and servers which collect, manage, and provide access to data. Ex: IT or Network Engineers/Analysts, Data Base Admins, ETL resources etc.	• Maintaining of physical and system security as per data classification. • Complying with applicable Enterprise Services policies, standards and guidelines.
Data Analyst	Individual responsible for Performing data collection, collation, validation and analysis activities, including verifying data quality; Ex: Statisticians, Bio-Statisticians, Data Scientists , Business Analysts , Consultants etc.	• Implementing tools for data collection and analysis to support the work of multiple roles. • Assisting data providers for the delivery of data to the organization. • Supporting the development of a standardized data governance framework. • Supporting the development and maintenance of suitable technical environments for hosting the data management and analysis framework;
Data Users	Enable the use of data of an organization. A data user is anyone who extracts value from data . Ex: Statisticians, Bio-Statisticians, Data Scientists , Business Analysts, Consultants etc.	• Finding and extracting value from data sets using the data dictionaries and data catalogs. • Interacting with other members of data governance like custodians and business owners. • Bringing attention to data governance team with quality or credibility issues.

		• Following appropriate security measures to protect sensitive data.

Table 1 - Data Governances Roles and Responsibilities

6. DATA GOVERNANCE

6.1 Definition

Data governance comprises of overarching policies, processes, standards, and metrics which ensure data is created, processed, distributed, and used efficiently and effectively within an organization. An Effective data governance ensures that data is consistent , trustworthy and used as intended.

The MOHAP possesses a strong and robust enterprise Data Governance framework for meticulously managing its' vast volume of data spread across its numerous departments, facilities, centers and associated offices.

Data Governance also plays a pivotal role for MOHAP in the collection and sharing of key healthcare data to and from numerous Internal and External entities, Governmental Agencies, Private Companies, Emirate-wise Statistics Centers, Universities and others.

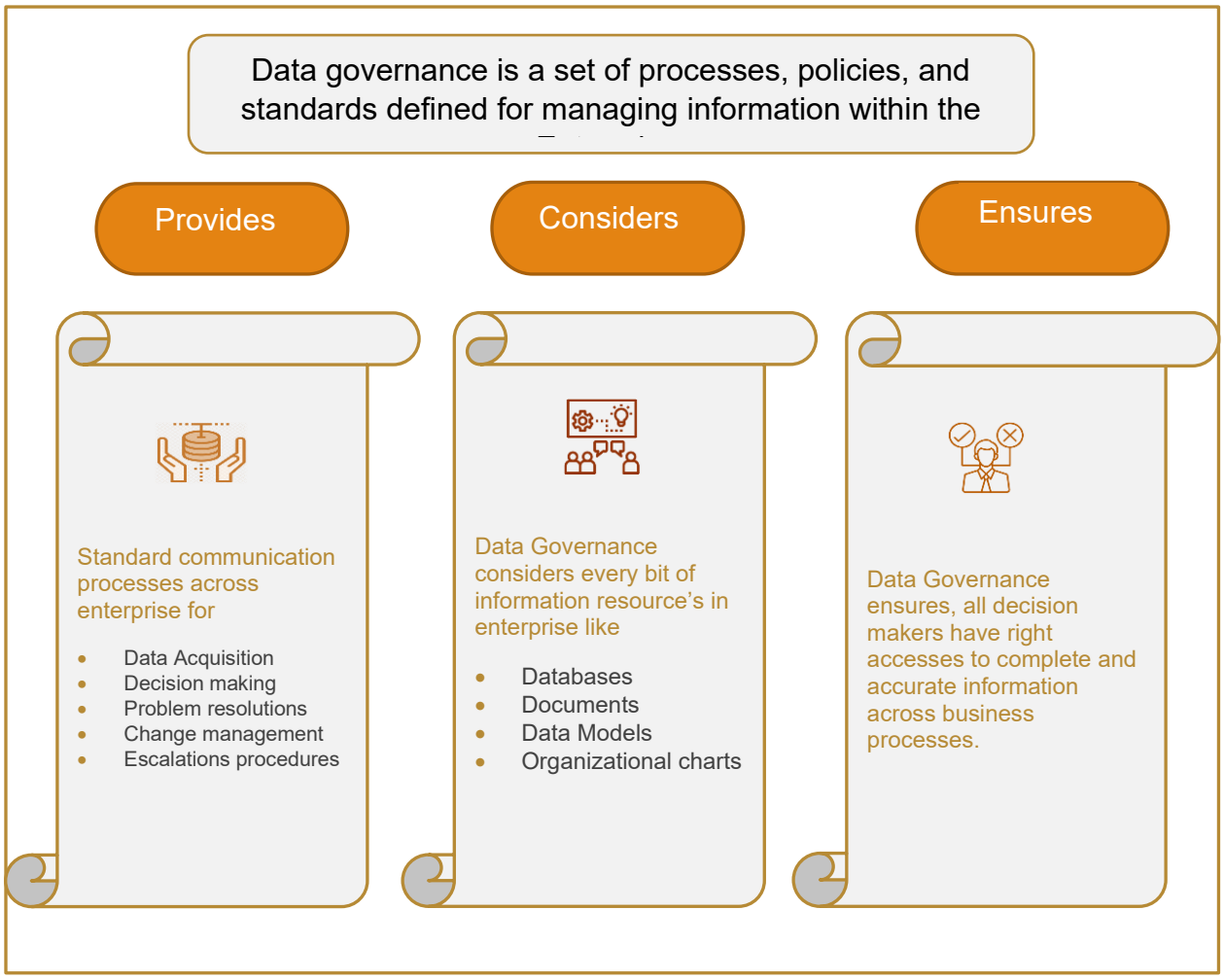


Figure 4 - Data Governance definition

6.2 Benefits

In general, the implementation of an enterprise data governance framework yields the below mentioned benefits for any organization;

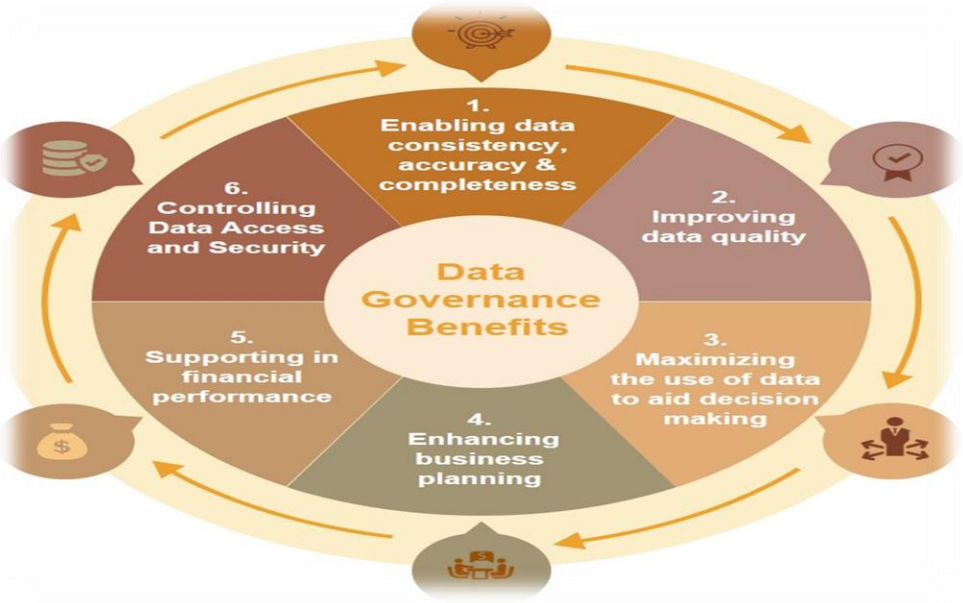


Figure 5 - Data Governance Benefits

The impact of above benefits from the MOHAP perspective is articulated below;

1. Possession of a vast ocean of rich and accurate Healthcare Data (Clinical, Statistical and Operational) at UAE level.

2. Astute interpretation , assessment and analytics of this data.

3. Utilization of this data for evidence-based policy decision-making.

4. Better planning in terms of health workforce, infrastructure, policies and health services for citizens

5. Identification of commercialization possibilities of this data indicating additional revenue streams.

6. Enforcement of restricted access, use and control of this data by identified internal and external stakeholder entities.

Figure 6 - MOHAP Data Governance Benefits

6.3 Framework

The below diagram reflects the MOHAP - Data Governance Organizational Framework comprising of the list of Key Governance Authorities, Internal and External stakeholders and Data Request/Approval flows.

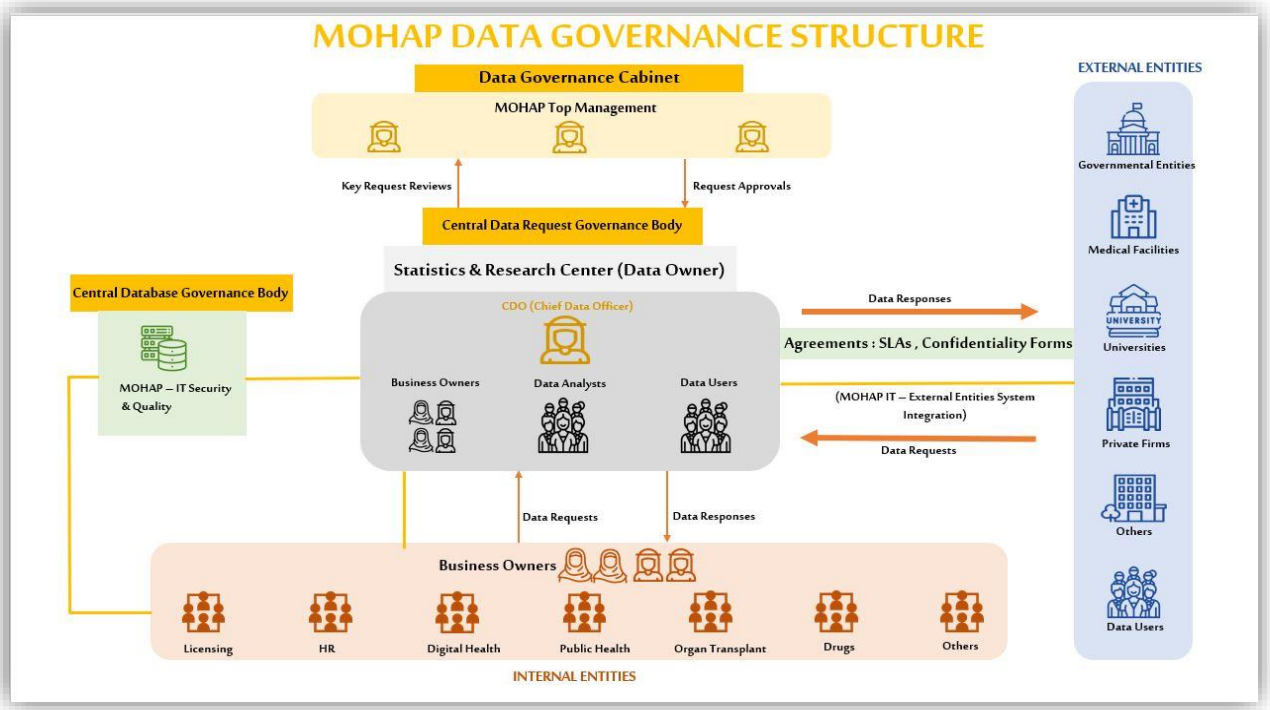


Figure 7 - MOHAP Data Governance Structure

1. Data Governance Cabinet

This cabinet consists of the MOHAP Top Management working in MOHAP with the aim of providing health care that is responsive to the needs of individuals and falling in line with the development and future vision of the state in all sectors and strives to be the world's best in all the services provided to people living in the UAE.

Key Data Governance Activities

Member	Chief Data Governance Role
MOHAP Top Management	Oversee all policies, laws and activities pertaining to Data Governance.
	Provide official Approval on sharing any data related to National Agenda, International Organizations and Newspapers/Media.
	Provide official Approval on sharing any data to Private Sector companies. Represent MOHAP in Service Level Agreements with external entities containing terms and conditions on data sharing.

Table 2 - Key Data Governance Cabinet

2. Central Data Request Governance Body

STATISTICAL & RESEARCH CENTER (SRC) is the chief **Data Owner ,** Custodian and Request Platform for all Healthcare based Clinical, Statistical and Operational data in UAE disseminated from MOHAP.

- The Director of this department serves the role of Chief Data Officer who is responsible for all the data within the organization as well as all data for UAE health across the country.
- The Section Heads of each Section in this department namely Statistics, Research, Disease Registry and Data Science & Informatics, play the role of Business Owners having the best subject matter expertise on their respective Data Sets and provide official approval on certain Confidential data.
- The Data Analysts/Users of this department essentially collect various Statistical Data from relevant internal and external entities across all emirates, with the ultimate goal of data aggregation and generating **UAE level data**. This is used for reporting in areas such as WHO core indicators, National Agenda 2021 indicators, Sustainable Development Goal indicators etc.
- As per the Ministerial Decree No 4259 of 2017 , The Statistics and Research Center (SRC) of MOHAP is the only entity authorized to review and approve all UAE level healthcare statistical, clinical or operational data before dissemination with other internal or external entities. **All MOHAP departments must respect all stipulations of this decree thereof.**
- A detailed SARC Request Workflow is present in Appendix section - 9.1 SARC Request Workflow which exactly describes the overall data request process;
    - Request Platform : All the requests related to statistics have to be requested through statistics section request email address (**sarc.request@mohap.gov.ae**).
    - Request Prioritization : The request received are prioritized by the handler depending on defined SRC guidelines for request priority. Every request received will be responded as per the defined priority.
    - Request Assignment : Received request has to be allocated to a particular section as per request type (statistics, research or national disease registry). The individual Section Heads are responsible to allocate the

required request to the personnel from their respective section. All the requests are required to be assigned to any particular staff within 24 hours from the receipt of the request along with the priority specified for the request. The staff in-charge of SRC will inform the requestor about the estimated time of completion for the request.

- Request Assignee Responsibility : Assigned person has to respond with the expected time required for resolving the request. In order to aid Data Quality and Consistency, Below steps are mandatorily performed;

  a) **Standard Report Template** : Once the data is ready, the staff has to conform to the official MOHAP - Government Communications format standards for Report Data is present in Appendix section - 9.3 SARC Report Template

  b) **Data Peer Review** : Thereafter the staff has to assign the request to another peer for peer review of the request resolution before sending response to the requestor.

- Request Management Review : For any request which requires sharing of confidential information, an approval is required before sharing this data with the requestor. The approval should be taken from the SRC Director and/or H.E. Undersecretary of the Ministry along with a confidentiality agreement which is required to be signed by the requestor's director or above level and shared back by the requestor to SRC. In case, no approval is provided by the requestor then the request will be refused and stands cancelled.

- Request Closure : Once the data is ready, It is incumbent upon the SARC.REQUEST team to thereafter share the final data with the requestor post validation and post approval process.

- As an example of Data Governance Journey, In the appendix section - 09.2 Data Governance Journey , SRC Sections - Statistics and Disease Registry data is present which contains the End to End Data workflow of each Data Set being worked on by the respective section, right from the **Data collection** from Source System, to **Data Processing/Aggregation** on received data, **Final Data** publishing and **Data Dissemination** to identified stakeholders.

3. Central Database Governance Body

As articulated in Data Architecture section, the Data from various Systems internal and external to MOHAP are extracted and stored in designated system-specific Databases which are governed by MOHAP-IT department. The MOHAP-

IT systems also have direct integration with couple of the External Entity systems such as Licensing, Birth & Death, HIS etc.

4. Internal Entities

These are various internal departments of MOHAP such as Licensing , HR , Public Health and Prevention etc. Each of these are custodians of their own local data however are obliged to share data on need-basis with SRC department as well as officially send their data requests to the SARC.REQUEST platform.

5. External Entities

These refer to those organizations which are such as outside the MOHAP ecosystem Governmental Entities Ex: DOH (Department of Health – Abu Dhabi), Private Companies, Universities etc. There are Service-Level agreements for data sharing signed between MOHAP and some of these External Entities which facilitate co-operation , compliance with relevant methodologies, support of statistical and research integration , provision of data-exchange framework and avoid duplication of statistical work performed.

In relation to Health Data Sharing, **MOHAP** is adhering to the Cabinet Resolution No. 32 of 2020 which is concerned with use of **Information and Communication Technology** in **Areas of Health**.
This is a **Health Data Law** centered around obligations for the collection, processing and transfer of health data by a broad range of entities within the UAE, including healthcare providers, health insurance providers, healthcare IT providers and providers of direct and/or indirect services related to the healthcare sector.
It has a series of articles pertaining to below areas;

- Definitions of Consent and Person's Identity Details;
- Health Authorities and Concerned Authorities joining the Central System
- Persons authorized to access the Central System
- Controls for permission to use the Central System
- Conditions and Controls for Using the Central System and Sharing Health Data and Information
- Controls for Saving Health Data and Information by Means of Information and Communication Technology
- Cancellations and many other aspects.

Additionally, The Service Level Agreements (SLAs) signed between **MOHAP** and **External Entities** typically highlight the adherence to the terms set in the SLA without prejudice to the inherent competencies of each entity across a series of articles pertaining to below areas;

SLA Area	Salient Features
Objectives	• SLA aims to establish closer statistical and research cooperation between the entities which complies with relevant methodologies, supports statistical and research integration across country and help prevent statistical work duplication. • Provide framework for exchange and reproduction of data. • Promote compliances with local and international methodologies, stands and data quality improvement. • Optimize use of administrative records in UAE.
Co-operation	For each Data Set there are certain co-operation/agreements between the entities; • Entities agree to co-operate in the exchange of data and information within stipulated time frames. • Entity 1 agrees to provide MOHAP data to facilitate identification of certain Key Health Indicators in UAE. • Raw Data for certain data set will be shared between both entities. • Entities shall provide data that facilities statistical work and caters to Urgent, Important and Adhoc requests.
Adhoc-Requests	• Request to be made within mechanism of cooperation. • Period of data availability shall be within 1-5 working days.
Data Exchange Properties	• Data will be exchanged securely through official shared folders , usb pen drive or email basis data size. • IT departments of each entity will be involved to ensure safety of data transmission.
Data Quality	• Both entities to agree on performing data checks for correctness and accuracy prior to sharing. • Written notification to be shared by either entity basis edit on shared data.

	• Data received by either entity to be checked for consistency and any gaps found shall be shared within 5 working days. • Entities will agree to provide metadata of data being shared.
Data Confidentiality	• Entities shall adhere to all regulations that protect confidentiality of data and ensure non-disclosure. • Confidential data will be treated by receiving entity with same care and diligence as that of own internal data.
Data Reproduction	• Data released by the entities is protected by copyright. Neither entity may fully or partially reproduce such data without written permission and source acknowledgment. • Both entities to respect flagging of data which is non-publishable and thus used only for internal purposes. • Entity who is not prime source of data will cite other entity as source in any publication or data release.
Co-ordination Arrangements	• Focal points will be nominated by each Entity for regular follow-up of SLA performance and assess commitment of each entity towards SLA terms. • Details of focal point such as Name, Designation, Phone and Mail shall be documented.
Dispute Handling	• Entities shall seek to amicably resolve any emergent disputes by first involving designated focal points and general coordinators. • Event of failure to resolve issue by focal points shall lead to representatives from each entity to jointly endeavor to resolve the issue. • If issue still persists then respective Board of Directors of each entity to get involved to resolve issue.
Notification	Any official correspondence among Entities shall be written in Arabic Language and addressed to the nominated focal points.

Amendments	• The entities may review and update present SLA basis request for either entity. • SLA update to come into effect only after written and signed agreement is completed by both entities.

Table 3 - SLA salient features

6.4 Ownership

In MOHAP, Data is gleaned from multiple external entities as well internally created. Thus, it is essential to explicitly define and state the ownership of this kind of data. A decree was also signed by the Undersecretary of the MOHAP, as an official policy to manage Data Ownership.

Below are the two types of Data Ownership possibilities related to the MOHAP Data Governance system;

a) MOHAP Ownership

- Any data which is created within any of the departments or facilities in MOHAP ecosystem is considered to have MOHAP Ownership. This data is safely stored in a secure shared-folder server with access provided to only those relevant individuals/roles who need to either review, work or share that data. As mentioned earlier ;

NOTE : Essential ownership of all UAE healthcare data lies with the Statistical and Research Department of MOHAP.

- If any externally sourced data is utilized for creating or modifying any MOHAP data then that external entity is mandatorily stated as an **official data source** for that data.
  For Ex: If Manpower Raw Data from Department of Health – Abu Dhabi (DOH) is utilized to calculated any particular indicator For Ex: Health Workforce Density; then its explicitly stated that DOH was the source for that data.

b) External Ownership

- Any data which is not created within the MOHAP ecosystem and has originated from any external entity ie. Governmental Entity, Private Company , Research Institute or Medical Company etc., is considered to have External Ownership**.** This data is typically obtained based on **Service Level Agreements (SLAs) or official agreements** signed with the concerned entities.

- Designated focal points of the external entities are responsible in disseminating their data in a timely and secure fashion with MOHAP. If their data is utilized AS-IS by MOHAP for any report, raw data or indicator calculation then that designated entity is explicitly credited as the Original Source for the data.

6.5 Policies

Policies related to Data Governance typically contain a set of rules for safeguarding Organization-wide data and establishing standards for the access , usage and integrity of this data. The chief purposes for this policy is to accentuate data criticality as well as promote a culture of data security involving active role of all stakeholders.

A policy document created by the SRC department named with document SARC Request Policy code# USO/Admin/138 can be found on MOHAP Open Data website. This is used as an example of the one of the core Data Governance Policy documents within MOHAP.

7. DATA QUALITY

7.1 Definition

Data Quality is a measurement of the condition of Data in terms of Consistency, Validity, Accuracy, Uniqueness, Timeliness and Completeness. On account of the continuously increasing volumes of diverse data present in MOHAP spread across its various departments, It is of utmost importance that this data is factually accurate, perspicuous , shareable and actionable for key decision-making and insights. Hence special focus is laid upon Data Quality in the entire MOHAP data ecosystem.

7.2 Dimensions

The Dimensions of Data Quality are a set of defined data measures which relate to multiple data attributes, records , tables , systems, sets etc. which help describe the quality of data existing in an organization. Below mentioned are the Key Dimensions which are considered in all undertaken practices throughout the process of handling data, from acquisition, to implementation, distribution and analysis.

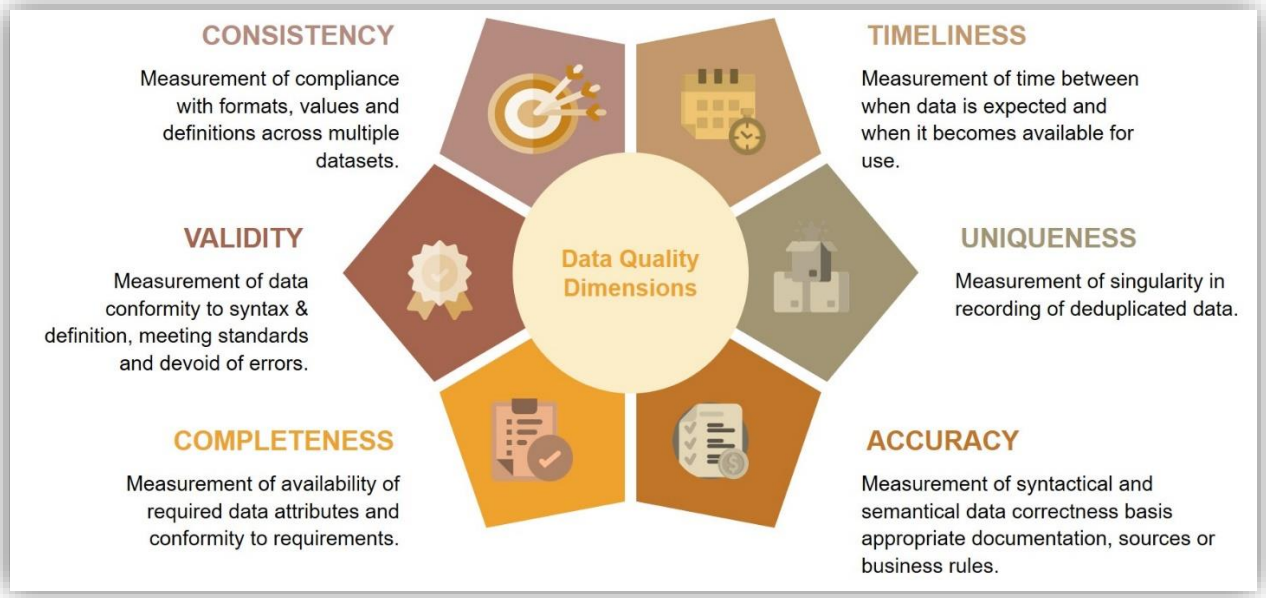


Figure 8 - Data Quality Dimensions

The Data Quality Indicators utilized in the SRC department as a reference which emphasizes the focus on Data Quality in MOHAP are present in Appendix section - 9.4 Data Quality Indicators.

7.3 Management Process

The comprehensive **MOHAP Data Quality Management Process** described below consists of

- Implementation - For continuous improvement of data quality.
- Data-Related Support - To enable implementation process by providing IT support .
- Resource Provision -To provide resources and training services.

Data quality management contributes to the processes, roles, standards, and metrics of data governance, helping to ensure the effective and efficient use of data in enabling an organization to achieve its goals.

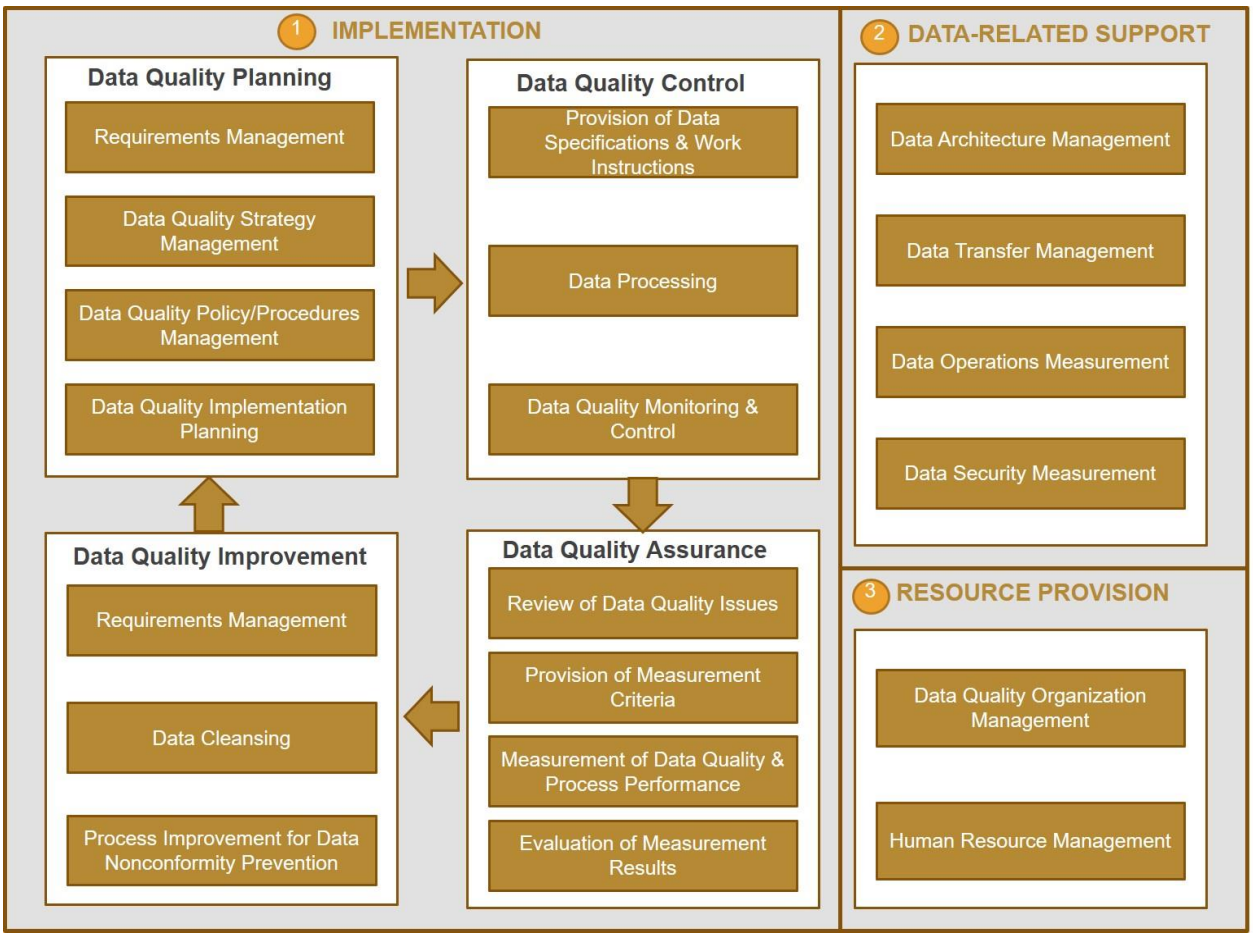


Figure 9 - Data Quality Management Process

7.3.1 Implementation Processes

Main-Process	Sub-Process	Overview
Data Quality Planning	**Overview**	It is bolstered by the existence of MOHAP Strategic Plan focusing on client requirements and continuous improvement of Data Quality Management System (DQMS). A set of detailed processes, policies, procedures, and plans have been created to detail the actions, levels, cost, resources, and capabilities required to achieve these objectives.
	Requirements Management	**Identification of Stakeholder** needs and expectation in terms of legal & regulatory requirements relevant to DQMS.
	DQ Strategy Management	**Definition of Data Quality (DQ) Strategy** with vision, long and short term goals, roadmaps etc. communicated through internal channels and outcome reviewed quarterly.
	DQ Policy/Standards/Procedure Management	**Documentation of Manuals** defining boundaries of DQMS, **Policies** towards strong DQMS, **Procedures** to support compliance with standards and **Forms** as evidence of implementation of documented procedures.
	DQ Implementation Planning	**Formulation of Plan** for Data Quality Implementation inclusive of DQ scope, target and resource allocation.
Data Quality Control	**Overview**	It is fostered by preparing implementation plan and processes that create, use and update data as per specific work instructions
	Provision of Data Specs. & Work Instructions	**Development of specifications** describing data characteristics used for Data Processing and Control through quarterly reports preparation.
	Data Processing	**Adoption of FCSC System** for performing data C.R.U.D operations in accordance with data specifications and work instructions.
	DQ Monitoring & Control	**Establishing DQ Monitoring and Control** basis Risk Identification, Analysis, Impact and Priority.
Data Quality Assurance	**Overview**	It is undertaken to measure Data Quality levels and process performance used as evidence to evaluate impact of poor data on business processes.
	Review of Data Quality Issues	**Initiation** – Responding to issues and non-conformities raised through data processing by internal or external stakeholders. **Analysis** – Review and investigation of above issues/non-conformities to find trends/patterns in non-conformity and to check if stakeholders needs are being met or not.
	Provision of Measurement Criteria	**Determination** of Data and processes measurement and **Development** of Key Performance Indicators and Measurement methods.

	Measurement of DQ & Process Performance	**Establishment** of measurement resources and Measurement of DQ levels and process performance levels.
	Evaluation of Measurement Results	**Analysis of measurement results** of data quality and process performance and Evaluation of their impact.
Data Quality Improvement	**Overview**	It involves analysis of the root cause behind data quality issues based on Data Quality assurance activities. The aim is to prevent future data issues by correcting current ones.
	Root Cause Analysis & Solution Development	**Analysis of root cause** of Each DQ issue and effect on business process is gauged. Thereafter solutions to eliminate root cause are proposed basis feasibility.
	Data Cleansing	**Correction of identified data non-conformities** in the available Data Set and development of actions to prevent recurrence of actual/potential non-conformities.
	Process Improvement for Data Non-Conformity	**Making improvements** to activities, outcomes and resources of processes and evaluation effectiveness of process improvements implemented.

Table 4 - Data Quality Management - Implementation Processes

7.3.2 Data Related Support Processes

Main-Process	Sub-Process	Overview
Data-Related Support	**Overview**	It provides the implementation process with Input data, Control Information and support for continuous improvement of Data Quality.
	Data Architecture Management	**Entailing exchange and sharing of organization-wide** common data and Management of organization-wide data-related artefacts to be used within MOHAP ecosystem.
	Data Transfer Management	**Recording of data transfers** for analysis and checking that data transfers meet applicable data specifications and work instructions.
	Data Operations Management	**Provision of environments** to ensure efficient processing of data and Management of data-related software and tools for data modelling, quality analysis and cleaning etc.
	Data Security Management	**Establishing of data security** criteria, management of data access authorization and audit of data security.

Table 5 - Data Quality Management – Data-Related Support Processes

7.3.3 Resource Provision Processes

Main-Process	Sub-Process	Overview
Resource Provision	**Overview**	It provides and controls organization resources required for the performance of Implementation and Data-Related Support.
	DQ Organization Management	**Establishing units supporting data quality** management and ensure important decisions on DQ issues are taken. Clear escalation process is established to ensure decisions are taken at correct organizational level. Documented data is also managed here.
	Human Resource Management	**Provision of data quality knowledge and skills**, data quality personnel and knowledge management.

Table 6 - Data Quality Management – Resource Provision Processes

7.4 Issues

Below mentioned are a set of general quality issues encountered whilst receiving data from external sources or at times even in internally created data items;

- **Incomplete data** : Laden with missing or blank items. **Ex:** Table/File having blank data under Gender field.

Table: Manpower

Name	Gender	Facility
Abdullah	Male	Hospital
Maryam		Clinic

- **Inaccurate data** : Which doesn't conform to the specified requirements. **Ex:** Data requested for Entry-Level Nurse however data received for Senior Nurses.

File 1: Expected Data

Name	Designation	Facility
Fatima	Junior Nurse	Hospital
Ameera	Nurse Intern	Clinics

File 2: Received Data

Name	Designation	Facility
Reem	Reg. Nurse	Hospital
Halima	Senior Nurse	Clinics

- **Invalid data :** Filled with erroneous or ambiguous content. **Ex:** Having data of Males in a Pregnancy related clinical data report.

File: Pregnancy Data

Name	Delivery Type	Mode of Delivery
Jamila	Spont.	Vertex
Khaled	Assisted	Breech

- **Obsolete data:** Data which is no longer valid. **Ex:** Latest data requested however received data older than 5 years.

File 1 : Expected Data

Emp ID	Designation	Year
1234	Sr. Consultant	2021
5678	Test Manager	2021

File 2 : Received Data

Emp Id	Designation	Year
1234	Consultant	2016
5678	Test Lead	2016

- **Duplicate data :** Multiple instances of same data in a single file. **Ex:** Multiple records of the same Employee with same Employee Id but different department details in a file.

File: Employee Data

EmpId	Name	Department
123	Salama	HR
123	Salama	Finance

- **Inconsistent data** : Data which is contradicted across multiple file versions.
Ex: Variance in data of patient across multiple files.

File 1

EmpId	Name	Nationality
1234	Ahmed	Egyptian
5678	Omar	Indian

File 2

EmpId	Name	Nationality
1234	Ahmed	Pakistani
5678	Omar	Jordanian

- **Data downtime :** Corruption in data on account of environmental or tool related issues.
Ex: Data sharing latency on account of environmental or server issues present with Source system.

7.5 Activities

Measures to eliminate Data Quality issues which were mentioned above are undertaken by all Data Governance Roles (as applicable) of each MOHAP Department. The typical activities carried out to ensure Data Quality are highlighted below;

Figure 10 - Data Quality Dimensions

In addition to above activities the final confirmation on the veracity of sensitive or critical data is provided by the Management Review in MOHAP either at Undersecretary or Department Director or Department Section Head level.
Basis which the final data is published and shared with external local and international entities.

Below is the mapping of above Data Quality Activities to the Dimensions of Data Quality;

Data Dimension	Data Quality Activity
Consistency	Planning , Auditing
Validity	Auditing , Standardization
Completeness	Updating
Timeliness	Conducting Meetings
Uniqueness	Cleaning
Accuracy	Peer Reviewing, Benchmarking

Table 7 - Data Quality Dimension - Activity Map

7.6 Metadata Management

5.6.1 Overview

Metadata management plays a pivotal role in MOHAP data governance by empowering all Data Users to derive value from the diverse and rich data sets they have at their disposal. Metadata is essentially data about data, which enriches the users with the information they need to add context to this data. Common metadata elements in data include title, description, tags, categories, author, modification dates, lineage, and more. Metadata management is a key component of data governance since it addresses many of the core issues that governance initiatives are designed to combat such as lack of standardization, ambiguous data ownership, undefined data quality rules, data security concerns, compliance concerns, an absence of lineage, communication issues, categorization problems, and more.

5.6.2 Examples

Below are existing examples of Data Dictionary files that facilitate Metadata management. Essentially these files contain the Numerator, Denominator, Reporting Frequency, Calculation Methodology , UAE /International Data Sources and numerous other relevant data for the gamut of Health Indicators calculated and reported by concerned departments in MOHAP.

Area	Description
WHO Core Health Indicators - Data Dictionary	This document provides the metadata definitions and year-wise values for the list of WHO Core Health Indicators which shall be used by the MOHAP in accurate calculation, documentation and eventual reporting of these indicator values.
All UAE Health Indicators - Data Dictionary	This document provides the metadata for all indicators calculated and reported by MOHAP namely WHO Indicators, National Agenda Indicators, Competitiveness Indicators, National Health Workforce Account indicators, ILO indicators and other Quality indicators. It can be found on **MOHAP Open Data** with document name - Health Indicators Data Dictionary.
Disease Registry Elements - Data Dictionaries	These documents provide the description and list of data elements/items across Disease Registries related to National - Injury & Poisoning , Diabetes, Cardiovascular and Cancer registries in UAE.

Table 8 - Metadata Data Dictionaries

7.7 ISO Certification

The **MOHAP** was awarded in the year **2021** with the International Organization for Standardization (ISO) Certificate of Compliance (ISO 8000-61:2016) towards **Data Quality Management**. This is a major milestone which signifies the excellent adherence to Data Quality Standards basis actual implementation of Data Quality measures by each department of this organization.

ISO 8000-61:2016
Data quality management - (1st federal government entity nationally to obtain this accreditation)

CERTIFICATE
of Compliance

This is to certify that the Data quality management: Process reference model requirements of

MINISTRY OF HEALTH AND PREVENTION.
Ministry of Health & Prevention, Muhaisnah 2, Mohammad Bin Zayed Road, P.O. Box 1853 - United Arab Emirates

Certificate No.: 21.67.AE401807.00
Original Approval: 10th April 2021
Certificate Issuance: 18th April 2021
Certificate Expiry: 17th April 2024
Re-Certification: 09th April 2024

Upon request from the management of MINISTRY OF HEALTH AND PREVENTION, W3 Solutionz has performed an independent assessment of the company's compliance against principles and contents of:

ISO 8000-61:2016

IN RESPECT TO THE PROVISION OF COMPREHENSIVE, INNOVATIVE, AND FAIR HEALTHCARE SERVICES AS PER INTERNATIONAL STANDARDS, AND PERFORMING THE ROLE OF HEALTHCARE REGULATOR AND SUPERVISOR THROUGH HEALTHCARE SUPPORT.

Director of Certification
ACS W3 Solutionz

In issuance of the certificate, ACS W3 Solutionz assume no liability to any other party other than to the client. This certificate becomes invalid if conditions of certification are not fulfilled (http://w3solutionz.com/doc/F-OPE-306CoP.pdf). This certificate is the property of W3 Solutionz FZE dba ACS W3 Solutionz, Off. M-02, Bldg: C-70, ME-10, Abu Dhabi – United Arab Emirates. Web: www.w3solutionz.com

04 - 220032

Figure 11 - Data Quality ISO Certificate

Overview : ISO 8000-61:2016 specifies the processes required for data quality management. The processes are used as a reference to enhance data quality and assess process capability or organizational maturity for data quality management.

It defines characteristics of information and data that determine its quality, and provides methods to manage, measure and improve the quality of information and data.

It specifies the processes required for data quality management. This specification is used as a reference for assessing and improving the capability of the processes or increasing organizational maturity with respect to data quality management.

It is intended for use by those actors that have a vested interest in information or data quality.

8. DATA SECURITY AND PRIVACY:

8.1 Definition

Data security consists of policies, procedures and processes for protecting data from unauthorized access, accidental loss and destruction. Whereas Data Privacy is an aspect of data protection that addresses the proper storage, access, retention, immutability and sharing of sensitive data. This section specifies the key aspects and implemented protocols for Data Security in MOHAP along with a snippet of the laws and policies pertaining to Data Security and Privacy.

Considering the MOHAP possesses a vast amount of sensitive clinical , administrative and operational healthcare data at UAE level, It is of paramount importance that this information be safely secured and protected from unauthorized access, malicious attacks and data exploitation. The data should also be disseminated only to trustworthy and intended recipients.

The Security and Quality Teams of MOHAP-IT department regulate and govern the entire MOHAP Data Ecosystem in terms of security and privacy. They maintain and processes information related to the organization, its employees, customers, and others who avail of its services. Recognizing the importance of the Information assets and the need for protecting them, they have implemented the Information Security Management System based on the international standards ISO 27001. They have also developed an Information Security Framework (described in below diagram) containing processes that define policies and procedures around the implementation and management of information security controls.

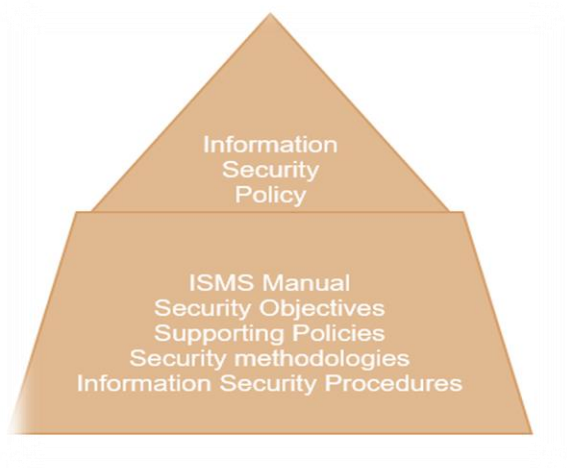


Figure 12 - MOHAP Information Security Framework

In general, below protocols related to IT Security are typically followed;

- **Password Management and Two-Factor Authentication**
  Utilization of strong Password Managers to help set strong/unique passwords across different devices.
  Enforcing multi/two factor authentication for all accounts to ensure authorized entry into the MOHAP network.

- **Email Vigilance**
  Guiding employees to be aware of suspicious requests, attachments, links, forged sender identities etc.

- **Phishing Awareness**
  Educating the employees in checking the sender of an email or look at URLs/attachments before clicking and informing MOHAP-IT in case of any suspicious mails/links.

- **Employee Training**
  Teaching the employees about social engineering and tactics which are used by professional hackers/scamsters to exploit vulnerabilities in human nature. This will lead to employees making better informed decisions related to secure usage of their systems and authorized access to various areas in the MOHAP network.

- **Avoiding Personal Devices at work**
  Recommending the employees to use designated laptops provided by MOHAP IT for official uses and avoid usage of personal devices such as laptops, usb drives , external hard disks etc. in office premises.

- **Using VPNs**
  Enforcing the safe access of MOHAP online infrastructure at homes by mandating download and usage of official MOHAP VPN on home network.

- **Strong Firewalls**
  Enhancing cyber security by implementing strong firewalls which can identify and control applications on any port, control circumvention , scan for viruses , generate alerts and control to-and-fro network traffic.

8.2 Key Aspects

There are three core elements to data security, namely Confidentiality , Integrity and Availability. These concepts are also referred to as the CIA Triad, functioning as a security benchmark model and framework for top-notch data security. Here's what each core element means in terms of keeping sensitive data protected from unauthorized access and data exfiltration.

Figure 13 - CIA Triad

The Federal Laws in relation to ICT(Information Communication Technology) in health fields drafted by the UAE President lays special emphasis on the Confidentiality, Availability and Integrity aspects of data.

Likewise, MOHAP has developed their data security protocols focusing on Data Sharing, Data Storage and Data Access as well as formulated key security policies on the basis of the CIA model.

8.3 Protocols

The protocols mentioned here are the actually implemented steps undertaken chiefly by the MOHAP-IT Security team for ensuring Data Security and Protection across the entire MOHAP ecosystem. These measures are in line with the associated Federal Law and Policies.

Below are the typical Security Measures undertaken by the MOHAP-IT Security Team across 3 pivotal areas of Data namely – Storage, Access and Sharing.

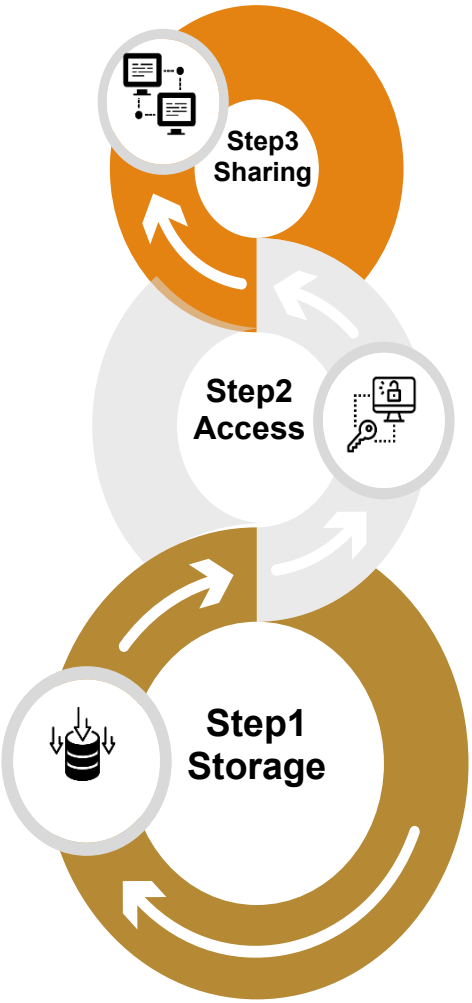


Figure 14 - Security Measures

Area	Security Measures
Data Sharing	Password-Protection on files being shared externally and internally.
	Secure file transfer system recommended for external data sharing.
	Email security gateway used to monitor all the information passed through email.
	USB ports disabled on all user system unless it is approved by the management.
	Audit tools used for file servers auditing.
Data Access	Access to information managed through identity and access management system.
	User accounts do not have privilege accesses. For privilege access, users use separate account which is managed through privilege access management solution.
	User accounts reviewed on regular basis.
	Vendor accounts reviewed on monthly basis.
	Use of non-default passwords enforced adhering with MOHAP security policy and disable default account wherever applicable.
	Role based access controls for data implemented.
Data Storage	Enforcement of data storage on centralized storage servers.
	Back-up of storage servers on daily basis and utilization of strong encryption.
	Updating version of all devices including servers and storage dedicated to MOHAP with the most recent OS, applications and antivirus version and its patches.
	Implementation of Database Hardening.
	Audit and monitoring of sensitive data.
	Usage of Non-default ports and named instances.

Table 9 - Security Measures

8.4 Federal Law

Information and communication technology (ICT) plays an integral role in supporting the delivery of quality healthcare services through the provision of new and efficient ways of health data access, communication, usage and storage.

Accordingly, The UAE passed **Federal Law No 2/2019 (ICT Health Law)** which regulates the use of Information and Communications Technology (ICT) in the UAE's health industry with below key aims;

- **Ensuring optimal use of information and communications technology in the health sector**
- **Ensuring bases, standards and practices adopted are in line with their internationally adopted counterparts**
- **Enabling MOHAP to collect, analyze and maintain health information at the country level**
- **Ensuring the security and safety of health data and information**

Figure 15 - ICT Law Aims

8.5 Policies

Information Security policies are high-level statements that provide agreed rules for strategic business related to data in an organization. The below policies are designed to be followed in the organization to reduce the critical risks from the data threats and unauthorized access which is not properly managed. The evidences for below policies are present in Appendix Section - **9.8 MOHAP Security related Policies**

Policy	Objective	Salient Features
Information Security Policy	Provides direction for the formulation, implementation and management of Information Security for MOHAP.	• Information Security Framework • Information Security Policy statement
Password Policy	Establishes the necessary security controls of user credentials for accessing any information system.	• Password management systems • Password communication • Password History Policy • User account-lock policy • Password composition and reset policy
Asset Management Methodology	Defines the methodology for identification, valuation, classification, labelling and handling of information assets.	• Asset Identification • Asset Recording • Asset Valuation • Asset Labelling • Information Asset handling
Internet and Email Policy	Regulates appropriate usage of Internet and Email for legitimate business purposes and protects MOHAP information assets from related threats and risks.	• Internet Policy Statements • Email Policy Statements
Encryption and Key Management Policy	Ensures that encryption keys are secured and managed throughout the life cycle. Encryption includes: windows logon, remote access, sensitive data encryption, emails, document encryption, application single sign-on, and web application logon.	Policy Statements: • General • Key Size & Algorithm • Administration & Key Management
Network Security Policy	Establishes security requirements for managing MOHAP's internal and external network for appropriate and secure operations of the information processing facilities and protect the confidentiality,	• Network Security Policy • Baseline Network Security • Network Segregation • Third Party Access • Network Infrastructure

	integrity and availability of data flowing through MOHAP's networks.	• Change Management Procedures • Network Risk Assessment
Secure Development Policy	Defines the policy related to secure software development and maintenance. It is a well-accepted principle that security should be considered at the design stage of the application or service and not at the delivery stage as an after-thought.	• Secure System Engineering • Secure System Development • Project Management • Outsourced Development • System Security Testing
Back and Restore Policy	Ensures that information systems and business applications are protected and recoverable in case of data corruption or system failure.	• Backup Policy for KDC Virtual Machines • Backup Policy for Hospitals Virtual Machines • Exchange 2010 and 2016 Emails • SQL Database • Oracle Database
Risk Management Methodology	Defines the Risk Management Methodology for MOHAP with a view to ensuring that risks to business operations are mitigated to the extent possible	• Key Responsibilities • Alignment to best practices • Risk Management Workflow • Risk Management Process • Risk Monitoring, Review, Reporting

Table 10 - Information Security Policies

8.6 Data Confidentiality

Data confidentiality focuses on the protection of data against unintentional, unlawful, or unauthorized access, disclosure, or theft. Below are couple of areas in the MOHAP ecosystem wherein Data Confidentiality is implemented;

- **Confidentiality Form:**
  In the MOHAP-SRC Department, A designated mail handle named SARC REQUEST serves as the official platform for handling any data requests emanating from other MOHAP departments and External entities (Ex: DHA,DOH etc). Whenever a request is received by SARC REQUEST team, which is of a sensitive or confidential nature, A mandate is imposed on the requestor whereby they must fill a Confidentiality Form for indicating their acceptance of terms & conditions of data usage, providing reason(s) for needing such data and specifying details of desired data items. The form is added in Appendix Section - **9.5 SARC Confidentiality Form.**

- **Data Set - Confidentiality classification**
  Each department within MOHAP works on various subject-specific Data Sets. For each of these Data Sets, It is imperative on these departments to classify the Confidentiality levels and Access-Groups permissibility levels as per below table.

Area	Values	Description
Confidentiality Level	• Open	Data which is publicly available on MOHAP Open Data.
	• Internal	Data which needs Management Approval.
	• Confidential	Data which needs Confidentially form filled by Requestor and Management Approval.
	• Restricted	Data which needs Confidentially form filled by Requestor and Undersecretary Approval.
Access Group Level	• Public	**Data is accessible for all public.**
	• External Entity	**Data is accessible for MOHAP and External Entities (Ex: DHA,DOH)**
	• MOHAP	**Data is accessible internally for all MOHAP departments/facilities.**
	• MOHAP-SRC	**Data is accessible internally solely for MOHAP-SRC department.**

Table 11 - Data Confidentiality Areas

An example of above data maintained by the Statistics, Disease Registry and Research Sections of SRC department is present in Appendix section - **9.6 SRC Data Confidentiality Matrix.**

8.7 ISO Certification

The **MOHAP** was awarded in the year **June 2022** with the International Organization for Standardization (ISO /IEC 27001:2013) towards **ISMS (Information Security Management System).** This is to certify that the Systems used for Providing IT services to the internal units and external entities are under the control of MOHAP as per SOA V1.2.

ISO 27001
Information security management

LRQA

Current issue date: 24 June 2022
Expiry date: 23 June 2025
Certificate identity number: 10453488

Original approval(s):
ISO/IEC 27001 - 24 June 2022

Certificate of Approval

This is to certify that the Management System of:

Ministry of Health & Prevention

Muhaisanah 2Sheikh Mohammed Bin Zayed RoadNext to Etisalat Academy, Sheikh Mohammed Bin Zayed Road,
Next to Etisalat Academy, Dubai, United Arab Emirates

has been approved by LRQA to the following standards:

ISO/IEC 27001:2013

Approval number(s): ISO/IEC 27001 – 00036604

The scope of this approval is applicable to:

ISO/IEC 27001:2013
Information Security Management System covering the systems and infrastructure at the Head Quarter of MOHAP, used for providing IT services to the internal business units of Ministry of Health and Prevention and to external entities as per SOA V1.2 dated 14-4-2022

Luis Cunha

Area Operations Manager - SAMEA

Issued by: LRQA Limited

UKAS MANAGEMENT SYSTEMS 0001

LRQA Group Limited, its affiliates and subsidiaries and their respective officers, employees or agents are, individually and collectively, referred to in this clause as 'LRQA'. LRQA assumes no responsibility and shall not be liable to any person for any loss, damage or expense caused by reliance on the information or advice in this document or howsoever provided, unless that person has signed a contract with the relevant LRQA entity for the provision of this information or advice and in that case any responsibility or liability is exclusively on the terms and conditions set out in that contract.
Issued by: LRQA Limited, 1 Trinity Park, Bickenhill Lane, Birmingham B37 7ES, United Kingdom

Page 1 of 1

Figure 16 - Data Security ISO Certificate

Overview: ISO/IEC 27001-2013 helps the organizations to protect their information in a systematic and cost-effective way which gives a trust to its customers and partners that it safeguards their data through the adoption of an ISMS.

It focuses on three aspects Confidentiality, integrity and availability.

It helps the organization to understand the various requirements of an information security management system and also manage information security risks implementing audit tools and risk assessments.

It is also invaluable in terms of monitoring, reviewing, maintaining and improving an organization ISMS.

9. APPENDIX

9.1 SARC Request Workflow

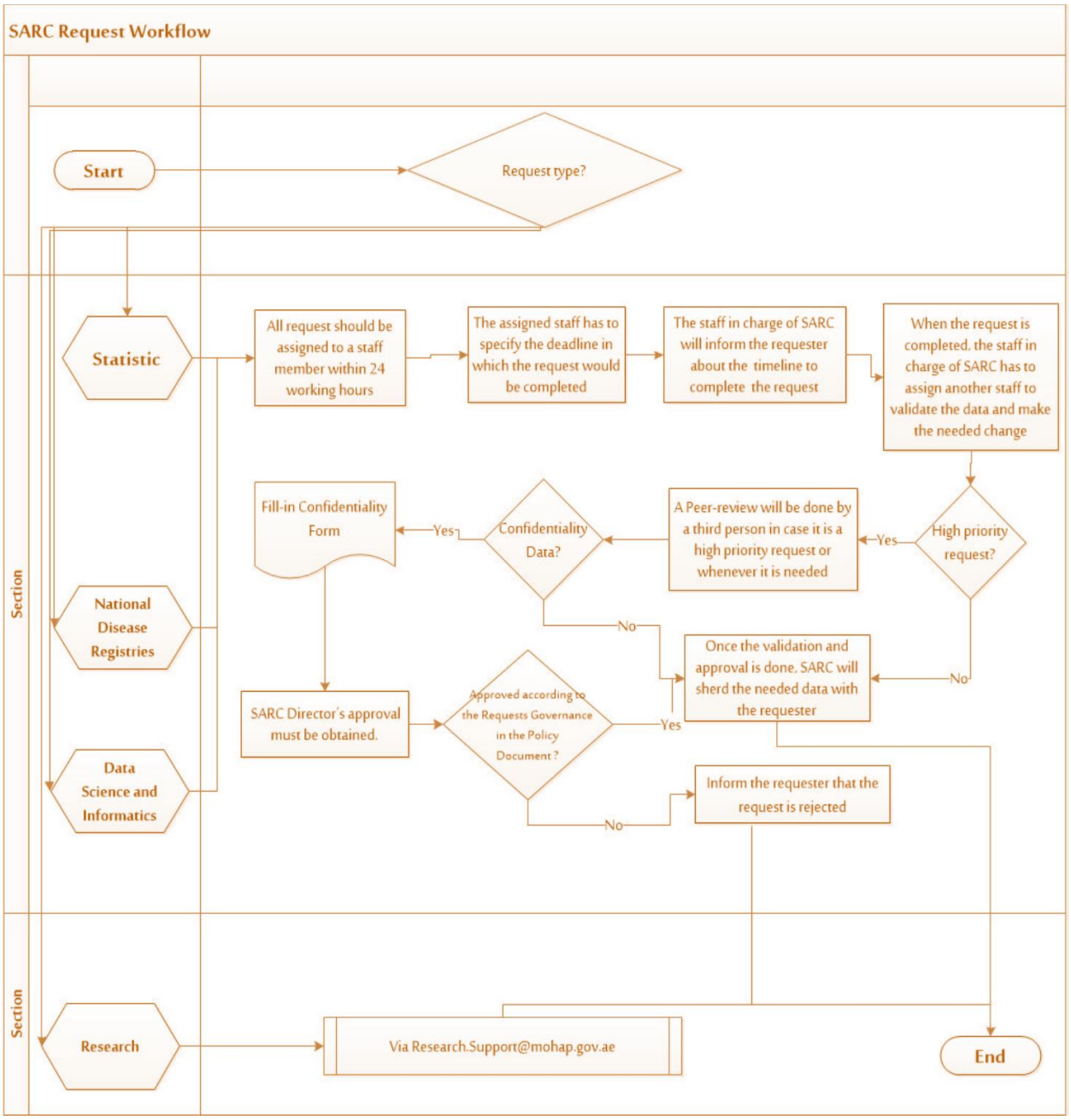


Figure 117 - SARC Request Workflow

9.2 Data Governance Journey

9.2.1 Statistics Data Governance Journey

Data Set	Type of Data	Source Data							Activities Performed on Data	Final Data			
		Name of Source	System Owner	Data Security	Data Receipt Process	File Format	Storage	Access		Storage	Confidential Access	Output	Stakeholders
		Name of Source System*	**Name of Entity Department that owns the System/ Data***	**Where source system data is stored**	**How is the source data sent to you**	**File format of Source Data**	**Where is data stored	**Who has access to this data which is sent by source**	**Which are the typical activities you perform on this Source data ,Eg - Cleaning, Standardization, Aggregation etc. Give example** , Objective = to create Final Data	**Where is final data stored	**Who has access to this final data	**Based on this final data are any other reports, KPI or other items created?...Name them**	**With which entities do you typically share this final data or report or KPI***

Births – Live and Still	Raw Data	Births System	MOHAP - Public Health Dept	DB (MOHAP-IT)	Email (Sent by MOHAP-IT)	Excel Raw Data	SHARED FOLDER	Senior Biostatistician	Activities mentioned in Data Quality Manual	SHARED FOLDER	Senior Biostatistici-an	UAE Births Raw Data File Report of UAE Births-Live and Still	WHO Tarkeeb Asukaniya
	Report	MOHAP SARC/ Open Data	MOHAP - SARC	MOHAP Open Data	NA	PDF	MOHAP Open Data	Universal	Activities mentioned in Data Quality Manual	SHARED FOLDER	Universal	Report of UAE Births-Live and Still	Report is shared on adhoc basis by SARC Request MOHAP Open Data - Different type of ppl who can access open data - researchers , students, governmental entities FCSC
Deaths by Cause of disease	Raw Data	Deaths System	MOHAP - Public Health Dept	DB (MOHAP-IT)	Email (Sent by MOHAP-IT)	Excel Raw Data	SHARED FOLDER	Senior Biostatist-ician Data Analyst	Activities mentioned in Data Quality Manual	SHARED FOLDER	Senior Biostatistician Data Analyst	UAE Deaths Raw Data File Report of UAE Deaths Core Indicators Calculated	WHO Tarkeeb Asukaniya Eg FCSC

Mortal -ity (New born, Neo-natal, Under 5 yrs)	Report	MOHAP SARC/ Open Data	MOHAP - SARC	MOHAP Open Data	NA	PDF	MOHAP Open Data	Universal	Activities mentioned in Data Quality Manual	SHARED FOLDER	Universal	Report of UAE Deaths	Report is shared on adhoc basis by SARC Request MOHAP Open Data - Different type of ppl who can access open data - researchers , students, governmental entities FCSC
WHO Core Indicators / Regional Core Health Indicators/ SDG and UHC Indicators	Report	Death and Birth DB for communicable diseases Sphere System (Future) HIS systems of all Entities Licensing System National Health Survey School Health Survey	Multiple Entities	HIS - each entity own system db D&B - MOHAP IT Licensing - MOHAP IT Currently DB for communicable disease - local system of Public Health dept	Licensing Team extract data from Lic System ie Facilities and Manpower Births & Deaths - email HIS data - Raw Data through emails Comm Diseases - pub health extract report from excel sheet and mail to us Sphere - future - will replace above excel sheet	Excel Raw Data	SHARED FOLDER	All raw data - All statisticia n	Activities mentioned in Data Quality Manual	SHARED FOLDER	All raw data - All statistician	WHO Core Indicators Yearly Report	WHO (WHO Data Portal) MOHAP Open Data

Health National Agenda Indicators	Report (Every 5 years)	Same as WHO Core Indicator										National Agenda Core Yearly Report	Not shared with WHO PMO National Program Manager of MOHAP
Hospital Services (Inpatient, Outpatient) per Emirates	Report	HIS System per entity	Each Entity's HIS dept	Each Entity's DB	Email (Sent by Each Entity)	Excel Raw Data	SHARED FOLDER	Statistician Bio Statistician	Activities mentioned in Data Quality Manual	SHARED FOLDER	Statistician Bio Statistician	Hospital Service Report Bed Study Statistical Annual Report. Report published on Open Data Indicators - WHO Core Indicator	FCSC
Bed Numbers Per Emirates		HIS System per entity	Each Entity's HIS dept	Each Entity's DB	Email (Sent by Each Entity)	Excel Raw Data	SHARED FOLDER	Statistician Bio Statistician	Activities mentioned in Data Quality Manual	SHARED FOLDER	Statistician, Bio Statistician	Bed Study Measure Occupancy Rate Indicator	

NHWA Indicators	Report	MOHAP Licensing System Central Higher Education Data Store Finance System of each Entity HR-Payroll System of each Entity	Multiple Entities governing their Licensing, Finance and HR data Central Higher Education Data Store (Ministry of Education)	Each Entity's DB/System	Email (Sent by Each Entity) Manpower and Facilities data extracted from Licensing System	Excel Raw Data and Report Data	SHARED FOLDER	Business Analyst	Activities mentioned in Data Quality Manual	SHARED FOLDER	Business Analyst	Numeric Indicators of National Health Workforce Account UAE Annual Report	WHO (WHO Data Portal) MOHAP Open Data
Manpower Statistics	Raw Data	MOHAP Licensing System	MOHAP-Licensing	Lic System DB (Lic Dept and IT)	Data extracted from MOHAP-Licensing System. This Lic System is integrated with Lic System of all entities. Mohd has direct access to this system,	Excel raw data	SHARED FOLDER	Data Analyst Senior biostatistician	Activities mentioned in Data Quality Manual	SHARED FOLDER	Data Analyst Senior biostatistician	UAE Manpower Report - Yearly NHWA Indicators calculated WHO Core Indicator Statistical Annual Report	

	Report	MOHAP SARC/ Open Data	MOHAP - SARC	MOHAP Open Data	NA	PDF	MOHAP Open Data	Universal	Activities mentioned in Data Quality Manual	SHARED FOLDER	Universal	NHWA Indicators calculated WHO Core Indicator Statistical Annual Report	
Facilities at UAE Level	Raw Data	MOHAP Licensing System	MOHAP-Licensing	Lic System DB (Lic Dept and IT)	Data extracted from MOHAP-Licensing System. This Lic System is integrated with Lic System of all entities. Mohd has direct access to this system,	Excel raw data	SHARED FOLDER	Data Analyst Senior Bio Statistici-an, Statistici-an	Activities mentioned in Data Quality Manual	SHARED FOLDER	Data Analyst Senior Bio Statistician, Statistician	UAE Facilities Report - Yearly NHWA indicator Statistical Annual Report	
	Report	MOHAP SARC/ Open Data	MOHAP - SARC	MOHAP Open Data	NA	PDF	MOHAP Open Data	Universal	Activities mentioned in Data Quality Manual	SHARED FOLDER	Universal	FCSC Annual Report NHWA Statistical Annual Report	FCSC WHO

Covid - Vaccination	Raw Data	Al Hosn (Ideal Data Source for all UAE data) HIS system per Entity	Each Entity's HIS dept	Each Entity's DB	Email (Sent by each Entity)	Excel raw data	SHARED FOLDER	Statistici-an Data Analyst Bio Statistici-an Business Analyst	Activities mentioned in Data Quality Manual	SHARED FOLDER	Statistician Data Analyst Bio Statistician Business Analyst	Covid Vaccination Daily Report - UAE level	NCEMA Dubai Police MOHAP -Internal Mgmt.
Communicable Disease	Report	Public Health Excel DB FUTURE - SPHERE, Usually Pub Health don't send raw data for Com Diseases	MOHAP - Public Health Dept	Public Health Excel DB	Email (Sent by MOHAP-Public Health)	Excel report data	SHARED FOLDER	Senior Bio Statisticia n	Activities mentioned in Data Quality Manual	SHARED FOLDER	Senior Bio Statistician	Calculate Communicable Disease Indicators Communicable Disease Report WHO Core Indicator Statistical Annual Report	WHO Open Data
Mental Health Data	Report	HIS System per entity	Each Entity's HIS dept	Each Entity's DB	Email (Sent by each Entity)	Excel report data	SHARED FOLDER	Bio Statisticia n	Activities mentioned in Data Quality Manual	SHARED FOLDER	Bio Statistician	Mental Health Indicators Mental Health Atlas Survey National Health Indicator Mental Health related Manpower Drug Addiction Indicators	WHO Internally - Program Manager of Mental Health

Malpra-ctice indicators	Report	Committee in each entity collects data	Each Entity's Concerned dept	Each Entity's DB/System	Email (Sent by each Entity)	Excel report data	SHARED FOLDER	Senior Bio Statistician	Activities mentioned in Data Quality Manual	SHARED FOLDER	Senior Bio Statistician	Malpractise Report UAE Rate of Malpractise per 10000 National Agenda Indicator	MOHAP - Strategic Department
Foreign Patients treatment in UAE	Report	HIS System per entity	Each Entity's Concerned dept	Each Entity's DB/System	Email (Sent by each Entity)	Excel report data	SHARED FOLDER	Any Statistician	Activities mentioned in Data Quality Manual	SHARED FOLDER	Any Statistician	Total Number of Patients per Nationality in each entity - Report	Ministry of Foreign Affairs
Insurance indicators	Report	Insurance Authority - UAE	Not Known	Not Known	Email	Excel report data	SHARED FOLDER	Data Analyst Senior Bio Statistician	Activities mentioned in Data Quality Manual	SHARED FOLDER	Data Analyst Senior Bio Statistician	% of Insured - Local and Non- Local in UAE per emirate National Agenda Indicator	MOHAP - Strategic Department

Universal Health Coverage	List of Indicators	Death and Birth DB for communicable diseases Sphere System (Future) HIS systems of all Entities Licensing System National Health Survey School Health Survey	Multiple Entities	HIS - each entity own system db Sphere - Not sure D&B - MOHAP IT Licensing - MOHAP IT Currently DB for communicable disease - local system of Public Health dept	Licensing Team extract data from Licensing System (Facilities and Manpower) Births & Deaths through email HIS data - Raw Data through emails Comm Diseases - pub health extract report from excel sheet and mail to us Sphere - future - will replace above excel sheet…..	Excel report data	SHARED FOLDER	All Statisticians	Activities mentioned in Data Quality Manual	SHARED FOLDER	All Statisticians	List of UHC Indicators	MOHAP - Health Services Planning and Health Economics Department

9.2.2 Disease Registry Data Governance Journey

Data Set	Type of data	Source Data							Activities Performed on Data	Final Data			
		Name of Source	System Owner	Data Security	Data Receipt Process	File Format	Storage	Access		Storage	Confidential Access	Output	Stakeholders
UAE National Diabetes Registry	Raw data (According to Data Dictionary)	Riayati system All private healthcare providers (Hospitals, Clinics), Labs treatment abroad mortality data DOH, DHA Central registries EHS facilities	MOHAP - Statistics and Research Center (Disease Registry Section)	Password / Encrypted files	Files shared through mail	Excel files	PC	HIS Specialist National Diseases Registry Specialist Disease Registry Section Head	Data Standardization - Disease Types, Gender, Age etc. Data Aggregation based on raw data Used for UAE public health purposes, like disease control ,guide planning and evaluation of diseases control efforts, prevention, Screening and to find the causes of health outcomes and diseases in populations Calculating all indicators , KPIs and burden of disease Writing annual report Providing recommendations for disease control	PC	HIS Specialist National Diseases Registry Specialist Disease Registry Section Head	Calculating all indicators , KPIs and burden of disease Writing annual report Providing information and recommendations for disease control	WHO Private Companies, like pharmaceutical companies UAE Health Facilities Government Entities Researchers and physicians Media International Organizations Ministries

UAE National Multiple Sclerosis Registry	Raw data (According to Data Dictionary)	Riayati system All private healthcare providers (Hospitals, Clinics), treatment abroad mortality data DOH, DHA Central registries EHS facilities	MOHAP - Statistics and Research Center (Disease Registry Section)	Password / Encrypted files	Not Yet			Disease Registrar National Diseases Registry Specialist Disease Registry Section Head	Data Standardization - Disease Types, Gender, Age etc. Data Aggregation based on raw data Used for UAE public health purposes, like disease control ,guide planning and evaluation of diseases control efforts, prevention, Screening and to find the causes of health outcomes and diseases in populations Calculating all indicators , KPIs and burden of disease Writing annual report Providing recommendations for disease control	PC	Disease Registrar National Diseases Registry Specialist Disease Registry Section Head	Calculating all indicators , KPIs and burden of disease Writing annual report Providing information and recommendations for disease control	WHO Private Companies, like pharmaceutical companies UAE Health Facilities Government Entities Researchers and physicians Media International Organizations Ministries
UAE National Cancer Registry (including Cancer Screening for Breast, Colon and Cervix)	Raw data (According to Data Dictionary)	Riayati system All private healthcare providers (Hospitals, Clinics), pathology Labs treatment abroad mortality data DOH, DHA Central registries	MOHAP - Statistics and Research Center (Disease Registry Section)	Password / Encrypted files	Files shared through mail	Excel files	PC	National Diseases Registry Specialist Disease Registry Section Head	Data Standardization - Disease Types, Gender, Age etc. Data Aggregation based on raw data Used for UAE public health purposes, like disease control ,guide planning and evaluation of diseases control efforts, prevention, Screening and to find the causes of health outcomes and diseases in populations Calculating all	PC	National Diseases Registry Specialist Disease Registry Section Head	Calculating all indicators , KPIs and burden of disease Writing annual report Providing information and recommendations for disease control	WHO Private Companies, like pharmaceutical companies UAE Health Facilities Government Entities Researchers and physicians Media International Organizations Ministries

		EHS facilities							indicators , KPIs and burden of disease Writing annual report Providing recommendations for disease control				
UAE National CVD Registry	Raw data (According to Data Dictionary)	Riayati system All private healthcare providers (Hospitals, Clinics), treatment abroad mortality data DOH, DHA Central registries EHS facilities	MOHAP - Statistics and Research Center (Disease Registry Section)	Password / Encrypted files	Files shared through mail	Excel files	PC	Disease Registrar, National Diseases Registry Specialist, Disease Registry Section Head	Data Standardization - Disease Types, Gender, Age etc. Data Aggregation based on raw data Used for UAE public health purposes, like disease control ,guide planning and evaluation of diseases control efforts, prevention, Screening and to find the causes of health outcomes and diseases in populations Calculating all indicators , KPIs and burden of disease Writing annual report Providing recommendations for disease control	PC	Disease Registrar, National Diseases Registry Specialist, Disease Registry Section Head	Calculating all indicators , KPIs and burden of disease Writing annual report Providing information and recommendations for disease control	WHO Private Companies, like pharmaceutical companies UAE Health Facilities Government Entities Researchers and physicians Media International Organizations Ministries

UAE National Mental Health Registry	Raw data (According to Data Dictionary)	Riayati system All private healthcare providers (hospitals, Clinics) treatment abroad mortality data DOH, DHA Central registries EHS facilities Ministries	MOHAP - Statistics and Research Center (Disease Registry Section)	Password / Encrypted files	Not Yet	Not Yet		Disease Registrar, National Diseases Registry Specialist, Disease Registry Section Head	Data Standardization - Disease Types, Gender, Age etc. Data Aggregation based on raw data Used for UAE public health purposes, like disease control ,guide planning and evaluation of diseases control efforts, prevention, Screening and to find the causes of health outcomes and diseases in populations Calculating all indicators , KPIs and burden of disease Writing annual report Providing recommendations for disease control	PC	Disease Registrar, National Diseases Registry Specialist, Disease Registry Section Head	Calculating all indicators , KPIs and burden of disease Writing annual report Providing information and recommendations for disease control	WHO Private Companies, like pharmaceutical companies UAE Health Facilities Government Entities Researchers and physicians Media International Organizations Ministries
Disability Registry	Raw data (According to Data Dictionary)	Riayati system All private healthcare providers treatment abroad mortality data DOH, DHA Central registries EHS facilities , و النوادي و مدينة الشارقة للخدمات الإنسانية و	MOHAP - Statistics and Research Center (Disease Registry Section)	Password / Encrypted files	Files shared through mail	Excel files	PC	National Diseases Registry Specialist, Disease Registry Section Head	Data Standardization - Disease Types, Gender, Age etc. Data Aggregation based on raw data Used for UAE public health purposes, like disease control ,guide planning and evaluation of diseases control efforts, prevention, Screening and to find the causes of health outcomes and diseases in populations Calculating all	PC	National Diseases Registry Specialist, Disease Registry Section Head	Calculating all indicators , KPIs and burden of disease Writing annual report Providing information and recommendations for disease control	WHO Private Companies, like pharmaceutical companies UAE Health Facilities Government Entities Researchers and physicians Media International Organizations Ministries

		مؤسسة زايد العليا و زارة تنمية المجتمع							indicators , KPIs and burden of disease Writing annual report Providing recommendations for disease control				
UAE National Injury Registry	Raw data (According to Data Dictionary)	Riayati system All private healthcare providers treatment abroad mortality data DOH, DHA Central registries EHS facilities ,Ministries , Dubai Police	MOHAP - Statistics and Research Center (Disease Registry Section)	Password / Encrypted files	Not Yet	Not Yet		National Diseases Registry Specialist, Disease Registry Section Head	Data Standardization - Disease Types, Gender, Age etc. Data Aggregation based on raw data Used for UAE public health purposes, like disease control ,guide planning and evaluation of diseases control efforts, prevention, Screening and to find the causes of health outcomes and diseases in populations Calculating all indicators , KPIs and burden of disease Writing annual report Providing recommendations for disease control	PC	National Diseases Registry Specialist, Disease Registry Section Head	Calculating all indicators , KPIs and burden of disease Writing annual report Providing information and recommendations for disease control	WHO Private Companies, like pharmaceutical companies UAE Health Facilities Government Entities Researchers and physicians Media International Organizations Ministries

UAE National Birth defect (Congenital anomalies) Registry	Raw data (According to Data Dictionary)	Riayati system All private healthcare providers treatment abroad mortality data DOH, DHA Central registries EHS facilities	MOHAP - Statistics and Research Center (Disease Registry Section)	Password / Encrypted files	Not Yet	Not Yet	Not Yet	National Diseases Registry Specialist, Disease Registry Section Head	Data Standardization - Disease Types, Gender, Age etc. Data Aggregation based on raw data Used for UAE public health purposes, like disease control ,guide planning and evaluation of diseases control efforts, prevention, Screening and to find the causes of health outcomes and diseases in populations Calculating all indicators , KPIs and burden of disease Writing annual report Providing recommendations for disease control	PC	National Diseases Registry Specialist, Disease Registry Section Head	Calculating all indicators , KPIs and burden of disease Writing annual report Providing information and recommendations for disease control	WHO Private Companies, like pharmaceutical companies UAE Health Facilities Government Entities Researchers and physicians Media International Organizations Ministries
UAE National Chronic Respiratory Registry	Raw data (According to Data Dictionary)	Riayati system All private healthcare providers treatment abroad mortality data DOH, DHA Central registries EHS facilities	MOHAP - Statistics and Research Center (Disease Registry Section)	Password / Encrypted files	Not Yet	Not Yet	Not Yet	National Diseases Registry Specialist, Disease Registry Section Head	Data Standardization - Disease Types, Gender, Age etc. Data Aggregation based on raw data Used for UAE public health purposes, like disease control ,guide planning and evaluation of diseases control efforts, prevention, Screening and to find the causes of health outcomes and diseases in populations Calculating all	PC	National Diseases Registry Specialist, Disease Registry Section Head	Calculating all indicators , KPIs and burden of disease Writing annual report Providing information and recommendations for disease control	WHO Private Companies, like pharmaceutical companies UAE Health Facilities Government Entities Researchers and physicians Media International Organizations Ministries

									indicators , KPIs and burden of disease Writing annual report Providing recommendations for disease control				
UAE National Kidney Registry	Raw data (According to Data Dictionary)	Riayati system All private healthcare providers treatment abroad mortality data DOH, DHA Central registries EHS facilities	MOHAP - Statistics and Research Center (Disease Registry Section)	Password / Encrypted files	Not Yet	Not Yet	Not Yet	National Diseases Registry Specialist, Disease Registry Section Head	Data Standardization - Disease Types, Gender, Age etc. Data Aggregation based on raw data Used for UAE public health purposes, like disease control ,guide planning and evaluation of diseases control efforts, prevention, Screening and to find the causes of health outcomes and diseases in populations Calculating all indicators , KPIs and burden of disease Writing annual report Providing recommendations for disease control	PC	National Diseases Registry Specialist, Disease Registry Section Head	Calculating all indicators , KPIs and burden of disease Writing annual report Providing information and recommendations for disease control	WHO Private Companies, like pharmaceutical companies UAE Health Facilities Government Entities Researchers and physicians Media International Organizations Ministries

UAE National Organ Donation and Transplantation	Raw data (According to Data Dictionary)	Riayati system All private healthcare providers treatment abroad mortality data DOH, DHA Central registries EHS facilities	MOHAP - Statistics and Research Center (Disease Registry Section)	Password / Encrypted files	Not Yet	Not Yet	Not Yet	National Diseases Registry Specialist, Disease Registry Section Head	Data Standardization - Disease Types, Gender, Age etc. Data Aggregation based on raw data Used for UAE public health purposes, like disease control ,guide planning and evaluation of diseases control efforts, prevention, Screening and to find the causes of health outcomes and diseases in populations Calculating all indicators , KPIs and burden of disease Writing annual report Providing recommendations for disease control	PC	National Diseases Registry Specialist, Disease Registry Section Head	Calculating all indicators , KPIs and burden of disease Writing annual report Providing information and recommendations for disease control	WHO Private Companies, like pharmaceutical companies UAE Health Facilities Government Entities Researchers and physicians Media International Organizations Ministries

9.3 SARC Report Template

9.3.1 Cover Page

Statistics & Research Center		
Report Title	Report Name.....	
Report Description	Report Description and Summary Text.....	
Tab Summary (If Multiple Tabs)	**Tab Name**	**Tab Description**
	Tab 1 Name	Tab 1 Description Text.....
	Tab 2 Name	Tab 2 Description Text.....
	Tab 3 Name	Tab 3 Description Text.....
	Tab 4 Name	Tab 4 Description Text.....
	Tab 5 Name	Tab 5 Description Text.....
Author	<First Name> <Last Name> <Designation>	
Reviewed By	<First Name> <Last Name> <Designation>	

9.3.2 Report

Statistics & Research Center										
<Report Name> <Year>										
Main Column	**Sub Column 1**	**Sub Column 2**	**Sub Column 3**	**Sub Column 4**	**Sub Column 5**	**Sub Column 6**	**Sub Column 7**	**Sub Column 8**	**Sub Column 9**	**Sub Column 10**
<Value1>										
<Value2>										
<Value3>										
<Value4>										
<Value5>										

9.4 Data Quality Indicators

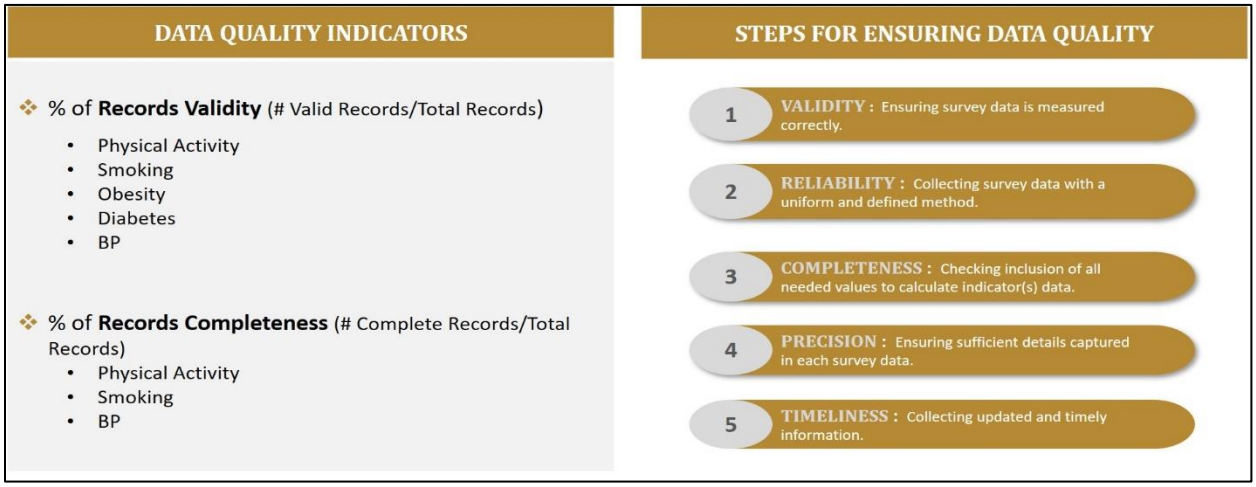
9.4.1 Statistics Section

DATA QUALITY INDICATORS	STEPS FOR ENSURING DATA QUALITY
❖ Weekly **COVID-19 death** related Indicators in COVID-19 Data Analysis EPI Week Report. ❖ Percentage of **SARC Request** tickets **Closed** On-Time. • 2020 : • 2021 : • 2022 : ❖ Percentage of **SARC Request** tickets **Peer Reviewed**.	1 **ACCURACY :** Cleaning of Data. 2 **COMPLETENESS :** Updating of missing records through verification from multiple systems. 3 **RELEVANCE :** Ascertaining whether data meets the requirements. 4 **DIVERSITY :** Collection of data from different entities country-wise. 5 **REVIEW :** Peer and Management Review of data as needed.

9.4.2 Disease Registry Section

DATA QUALITY INDICATORS	STEPS FOR ENSURING DATA QUALITY
❖ **Healthcare Providers** submitting required Disease Registry Data / Total **Healthcare Providers** **(Per Year)** ❖ Disease Registry **Workshops Implemented** / Disease Registry **Workshops Planned** **(Within Year)**	1 **INTERNATIONAL STANDARDS :** SEER,ICD,AJCC etc applied on DR Data. 2 **DATA DICTIONARY :** Created with detailed data items, definitions and rationale. 3 **EDIT CHECKS :** Applied on various documents. 4 **WORKSHOPS :** Conducted in collaboration with WHO. 5 **VERIFICATION :** Performed on de-duplicated clinical data by Qualified Cadre.

9.4.3 Research Section



9.5 SARC Confidentiality Form

SARC Data Request Form and Confidentiality Agreement

This document describes policies governing the release of data from Statistics and Research Center (SARC) at the UAE Ministry of Health and Prevention (MOHAP).

Kindly complete the form and you **must** indicate your acceptance of the terms and conditions by signing the Confidentiality Statement.

Reason for Request

☐ Media

☐ Public

☐ Disease Strategy Directorate

☐ Health Board

☐ Presentation: Kindly specify below:

- At United Arab Emirates, please specify: _____
- Outside United Arab Emirates, please specify place and the event: _____

☐ Publication: Kindly specify the name of the journal: _____

☐ Feasibility study for potential research project

☐ Administrative Decision

☐ Research project, please provide the following information:

- Ethical approval number: _____
- Ethical approval date: ____/____/____

☐ Others, please specify: _____

Information Requested (*Please specify type of information/data needed***):-** ----------
---

Confidentiality Statement

Terms and Conditions of released data

You must agree to the terms of use as set out below in order to receive data from MOHAP Statistic and Research Center (SARC). The data supplied to you remains the property of MOHAP. To protect against misuse of the data, all requestor must agree to the following conditions:

- MOHAP Statistics and Research Center is to be clearly acknowledged as the source of the data in any publication or presentation in which it is used.
- MOHAP Statistics and Research Center is to be sent a draft copy, prior to submission to any peer reviewed journal, of any paper based on SARC data.
- SARC may refuse permission for the use of the data in this way if this would not be in the interests of the UAE MOHAP.
- **No** presentation of the data which could potentially identify any individual patient, doctor or health care institution is to be made without the permission of SARC and of the person or institution concerned.
- Data released shall be only used for the purpose mentioned in this form.
- Any direct contact with the patients to collect additional or updated information is **prohibited**, unless it was explicitly approved by SARC or MOHAP Top Management.

I have read and understood the above rules and I agree to accept the responsibility for the Terms and Conditions of the released data.

Name _____

Organization/Department _____ **Occupation** _____

Signature _____ **Date** dd / mm / yyyy

For the Use of the Statistics and Research Center at MOHAP

Requester Name:	
Requester's Organization:	
Date Received:	
Date Issued:	
SARC Director's Decision	☐ **Approved** ☐ **Not Approved**
Comments:	
Signature	**Date:** dd / mm / yyyy

9.6 SRC Data Confidentiality Matrix

9.6.1 Guidelines

a) Confidentiality Selection

- **Open** - Data which is publicly available on MOHAP Open Data.
- **Internal** - Data which needs Management Approval.
- **Confidential** - Data which needs Confidentially form filled by Requestor and Management Approval.
- **Restricted** - Data which needs Confidentially form filled by Requestor and Undersecretary Approval.

b) Accessibility Group Selection

- **Public** - Data is accessible for all public.
- **External Entity** - Data is accessible for MOHAP and External Entities like DOH,DHA,MOPA etc.
- **MOHAP** - Data is accessible internally for all MOHAP departments/facilities.
- **MOHAP-SARC** - Data is accessible internally solely for MOHAP-SARC department.

9.6.2 Statistics Selection

Category	Task	Public	Protected	Restricted	Confidential	Access Group
1-Health Core Indicators	Core Indicators Report	*				Public
	Dashboards	*				Public
2- Sustainable Development Goals	Sustainable Development Goals Annual Report	*				Public
	Sustainable Development Goals Dashboards	*				Public
3- Competitiveness Indicators	Reports		*			MOHAP
	Dashboards		*			MOHAP
4- Birth Data	Raw Data				*	SARC
	Maternal & Child Indicators	*				Public
	Maternal & Child Reports (MOHAP Internal)			*		MOHAP
	Maternal & Child Reports (WHO)	*				Public
	Maternal & Child Dashboards		*			MOHAP
5- Mortality Data	Raw Data				*	SARC
	Mortality Indicators			*		MOHAP

	Mortality Reports (MOHAP Internal)			*		MOHAP
	Mortality Reports (WHO)	*				Public
	Mortality Dashboards			*		MOHAP
6- Communicable Diseases	Communicable Diseases Raw Data				*	SARC
	Communicable Diseases Indicators			*		MOHAP
	Communicable Diseases Reports (MOHAP)			*		MOHAP
	Communicable Diseases (WHO) & MARS	*				Public
	Communicable Diseases Dashboards			*		MOHAP
7- NCD Mortality Data	NCD Data Raw Data / Program Data				*	SARC
	NCD Indicators	*				Public
	NCD Reports (MOHAP Internal)			*		MOHAP
	NCD Report (WHO)	*				Public
8- Healthcare Services (IP,OP, ED) Data	Healthcare Services (IP,OP, ED) Raw Data			*		SARC
	Healthcare Services Reports	*				Public
	Healthcare Services Dashboards	*				Public
9- Healthcare Services (Beds)	Healthcare Services (Beds) Data	*				SARC
	Beds Indicators	*				Public
	Beds Report	*				Public
	Dashboards	*				Public
10- Statistical Annual Report	Statistical Annual Report	*				Public
11- Licensing Manpower	Raw Data				*	SARC
	Manpower Indicators	*				Public
	Manpower Reports (MOHAP)	*				Public
	NHWA (WHO)	*				Public
	Manpower Dashboards	*				Public
	NHWA Dashboards	*				Public
12- Licensing Facilities & Pharmacy	Raw Data				*	SARC
	Facilities Indicators	*				Public
	Facilities Reports (MOHAP)	*				Public

	Facilities Dashboards	*				Public
13- Insurance Data	Raw Data				*	SARC
	Indicators		*			MOHAP
	Insurance Reports (MOHAP)		*			MOHAP
14- Data Index*	Data Index		*			External Entity
15- Mental Health*	Raw Data				*	SARC
	Mental Health Indicators			*		MOHAP
	Mental Health Report (MOHAP)			*		MOHAP
	Mental Health Survey (WHO)	*				Public
	Mental Health Dashboards				*	MOHAP
16- Drugs Addiction Data	Raw Data				*	SARC
	Drugs Indicators				*	MOHAP
	Drugs Report (MOHAP)				*	MOHAP
17- Education Data (HRH)	Raw Data				*	SARC
	HRH Indicators		*			MOHAP
	Reports (MOHAP)		*			MOHAP
	HRH Dashboards	*				Public
18- Organ Transplant	The Reports (MOHAP)			*		MOHAP
19- Air Pollution Study*	Raw Data				*	SARC
	The Report			*		MOHAP
20- Aging Data*	Raw Data				*	SARC
	Aging Report	*				Public
	Aging Survey	*				Public
21- Neonatal Testing Data	Raw Data				*	SARC
	The Report (MOHAP)		*			MOHAP
22- Dialysis Data	Raw Data				*	SARC
	The Report (MOHAP)	*				Public
23- Fertility Data	Raw Data				*	SARC
	The Report (MOHAP)				*	MOHAP

24- Telemedicine & AI Topics	Collected Data		*			SARC
	The Report (MOHAP)	*				Public
25- HALE	Raw Data				*	SARC
	The Report (MOHAP)	*				Public
26- Immunization	Raw Data				*	SARC
	Immunization Indicators	*				Public
	Immunizations Reports (MOHAP)		*			MOHAP
	Immunizations Reports (WHO)	*				Public
	Immunization Dashboards	*				Public
27- Labour Medical Fitness	Raw Data				*	SARC
	Indicators	*				Public
	Reports (MOHAP)		*			MOHAP
	Dashboards	*				Public
28- Hospital Accreditation	Collected Data		*			SARC
	Indicators	*				Public
	Reports (MOHAP)		*			MOHAP
	Dashboards	*				Public
29- Malpractice Project	Raw Data				*	SARC
	Reports				*	MOHAP
30- Gender Balance File	Collected Data		*			SARC
	Reports & Indicators	*				Public
31- National Food Security Strategy	Raw Data				*	SARC
	Reports & Indicators			*		MOHAP
32- National Readiness Indicators	Indicators Results				*	MOHAP

9.6.3 Disease Registry Selection

Work Area	Public	Protected	Restricted	Confidential	Access Group	Note
Raw data of the National Disease Registries (identifiable)				*	MOHAP-SARC	Disease Registry team only
De-identified Raw data of the National Disease Registries			*		External Entity	Under Data Sharing Agreement
Aggregated Disease Registry Data (Non-identifiable)			*		External Entity	Under Data Sharing Agreement
Annual Disease Registries Reports	*				Public	
Research Datasets Derived from Registries			*		Public	Approved IRB
Disease Registry Dashboards (Aggregated Indicators)		*			MOHAP	
Disease Incidence Indicators	*				Public	
Disease Prevalence Indicators	*				Public	
Disease Mortality Indicators	*				Public	
Cancer Survival Indicators		*			MOHAP	
Trend Analysis and Forecast Indicators		*			MOHAP	

9.6.4 Research Selection

Work Area	Public	Protected	Restricted	Confidential	Access Group
NHNS Data			*		MOHAP-SARC
School Obesity Data			*		MOHAP-SARC
Research Bank	*				Public
WASH(Water, sanitization & Hygiene) SURVEY		*			MOHAP
Internal Surveys and Data Collection		*			MOHAP

9.7 MOHAP Application Topology

Id	Application	Application Name	Services	Objective	Business Owner Department	Business Owner	Business Driver	Users of the System	Integrations (External Entities)	Integrations (Internal Entities)
1	**Birth and Death System**	Birth and Death Notification system -Issue a Birth or Death certificate to general public based on the notification received from hospitals. UAE law for notification of B & D for national population registry.Adopting the strategy of the Government of UAE to have one centralized system incorporating all the stake holders which benefits in having One Stop Shop automated solution for birth and death data analysis that help putting health strategies and national level KPIs.	Issue Birth Certificate Issue Death Certificate Notification of Still Birth Issue Age Estimation Certificate	Adopting the strategy of the Government of UAE to have one centralized system incorporating all the stake holders which benefits in having One Stop Shop automated solution for birth and death data analysis that help putting health strategies and national level KPIs.	Preventive Medicine Dept (PMD)	Department Director	Regulatory / Customer experience / Revenue	All Hospitals Private & Govt , Preventive Medicine Dept (PMD), Statistics dept	1. ICP 2. MOJ 3. MOCD 4. FCSA 5. DHA 6. MOF 7. MOI 8. DoF 9. Empost	1. Wareed 2. SMS
2	**Chemical Precursors Import/Export and Company Registration with MOI**	Chemical Precursors Import/Export and Company Registration with MOI		Integration with MOI for Chemical precursor company registration and import/export of chemical precursor substances	Drug Control Department	Department Director	Regulatory	Business	1. MOI (Manafeth) 2. UAE PASS	
3	**Drug Import Export**	Drug Import Export System	Issue Import Permits Issue Export Permits	System to issue permits for import and export of medical products	Drug Control Department	Department Director	Regulatory	Medical Product Agents and Companies/factories	1. AD Customs 2. MoF eDirham 3. UAE PASS	
4	**Good Standing Certificate**	Good Standing Certificate System	Issue Good Standing Certificate	System to issue Good standing certificate for Medical professionals	Licensing & Accreditation Dept	Department Director	Regulatory	Medical Professionals	1. UAE PASS 2. MoF eDirham	1. Medical Licensing 2. Professional Licensing 3. SMS

5	**High Committee For Medical Liability system**	High Committee For Medical Liability system	High Committee For Medical Liability system	System to assess cases for the Higher committee for medical liability	Higher Committee for Medical Liability	Department Director	Regulatory, Compliance	High Committee For Medical Liability, Federal Authorities		1. Medical Licensing
6	**Mawardna**	Mawardna		Management of available medical resources for crisis and emergency center	Crisis & Emergency Department	Medical Practitioner	Operational Efficiency	Business/Hospital/ Health Authorities	1. NCEMA 2. Private Hospitals	
7	**Medical Advertisement and Violation System**	Medical Advertisement and Violation System	Issue Health Adevrtisement Licenses	System for registering medical establishments to license medical advertisements.	Licensing & Accreditation Dept	Department Director	Regulatory	Medical Professionals	1. MoF eDirham 2. UAE PASS	1. Medical Licensing 2. Professional Licensing 3. SMS
8	**Treatment Abroad**	Overseas Treatment Abroad System	Apply for Overseas Treatment services	System to apply for treatment abroad	Oversees Treatment Department	Assistant Undersecretary for External Relations and Health Affairs	Customer Experience	Citizens	1. ICP 2. DOH 3. DHA 4. UAE PASS	1. SMS
9	**Sick Leave Attestation**	Sick Leave Attestation	Apply for Sick leave attestation service	System for attessting the sick leaves and medical reports.	Licensing & Accreditation Dept	Department Director	Regulatory, Revenue	Public	1. ICP 2. MoF eDirham 3. UAE PASS 4. FAHR	1. Licensing System 2. SMS
10	**Pharmaceutical Licensing**	Pharmaceutical Facility and Professional Licensing	Pharmaceutical Facility and Professional Licensing	System for issuing licenses to pharmaceutical faclities and staff.	Licensing & Accreditation Dept	Department Director	Regulatory, Revenue	Pharmaceutical Facilities	1. MoF eDirham 2. MOI 3. UAE PASS	1. Evaluation System 2. SMS 3. Inspection System

11	**Medical Licensing**	Medical Facility and Professional Licensing	Apply for Medical Establishment Licensing Apply for Medical Professional Licensing services	System for issuing licenses to medical faclities and staff.	Licensing & Accreditation Dept	Department Director	Regulatory, Revenue	Medical Facilities	1. MoF eDirham 2. MOI 3. UAE PASS	1. SMS 2. Evaluation System
12	**Medical Professional Evaluation**	Medical Profession Evaluation System	Apply for Evaluation service	System for assessment for medical professionals such as Physicians, dentist, nursing, Allied and TCAM categories.	Licensing & Accreditation Dept	Department Director	Regulatory, Revenue	Medical Professionals	1. Prometric Testing Center 2. DataFlow 3. UAE PASS	1. Licensing System 2. SMS 3. Inspection System

9.8 MOHAP Security related Policies

9.8.1 Information Security Policy

1. Introduction

The IT&HIS department of Ministry of Health and Prevention (MOHAP) maintains and processes information related to the organization, its employees, customers, and others who avail of its services. Recognizing the importance of the Information assets and the need for protecting them, IT&HIS department intends to implement Information Security Management System based on the international standards ISO 27001.This document defines the Information Security Policy of IT&HIS Department of the Ministry of Health and Planning.

2. Purpose

The purpose of this document is to provide direction for the formulation, implementation and management of Information Security at IT&HIS Department of MOHAP.

3. Applicability

This Information Security Policy is applicable to all the information systems, assets, devices, employees and other personnel covered by the Scope of the Information Security Management System.

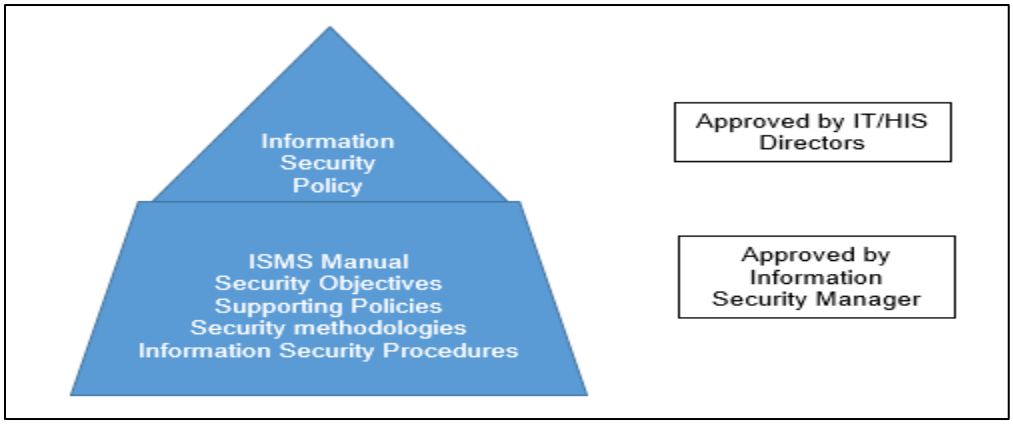
4. Compliance

Compliance to this Information Security Policy is mandatory for all the employees, contractors, consultants and other personnel covered by the scope of Information Security Management System. If any employee is aware of an information security incident he/she should report it immediately to IT Service Desk who will raise a case with Security team.

5. Key objectives

Information assets of IT&HIS Department shall be protected from threats to confidentiality, integrity and availability. The objectives of the management system are defined in the document “ISMS Objectives”.

6. Information Security framework



7. Information Security Policy statement

The management and employees of IT&HIS Department are committed to securing the confidentiality, integrity and availability of all the information assets, enhance the trust and confidence of all stakeholders and customers, and ensure compliance to statutory, regulatory and contractual requirements.

The goal of secure information system will be achieved by implementation of security policies and procedures, spread of information security awareness, periodic evaluation of security objectives, and conduct of internal audits, review and action on incidents, and planning and implementation of appropriate corrective actions, leading to a continual improvement of the management system.

9.8.2 Password Policy

1. Objective

The objective of this policy is to establish the necessary security controls of user credentials for accessing any information system.

2. Scope

This policy applies to all systems and applications on all system platforms that require user authentication (i.e. username and password).

3. Policy Details

- All privileged accounts internal systems and applications must have authentication password with minimum of 12 characters.
- All internal systems and applications must enforce regular password change.
- All public portals must have authentication password with a minimum of 8 characters
- Users shall use complex password.
- Users shall change their new passwords the first time they log on to the system.
- Users shall change their passwords on a regular basis at most every three months. Passwords for Service Accounts shall be configured as never expire and shall be changed by respective administrators at regular intervals.
- Users shall not write down their passwords or post them on their screens or desks.
- Users shall not disclose or share their passwords with others.
- If user password is disclosed for any system, users shall change it immediately.
- Password of Application Administration accounts will be known to MOHAP Applications Admins and should not be shared with System Admins.
- Users shall inform the concerned security team when suspecting any misuse of their credentials.
- Issues should be reported to SOC@mohap.gov.ae

4. Password Management Systems Requirement

- Enforce the use of individual passwords to maintain accountability.
- Allow users to select and change their own passwords
- Enforce alphanumeric password composition rules
- Force users to change temporary passwords at first login
- Require re-authentication prior to permitting a user to re-access an information resource after a period of inactivity
- Maintain a record of previous user passwords to prevent re-use
- Not provide specific feedback to the user if any portion of the login information is entered incorrectly
- Only indicate login failure after both the identifier and authentication information have been entered
- Display the number of unsuccessful login attempts made, since the last time the user successfully logged in.
- The password age should be set to minimum of 1 day this will ensure a set period of time that a password must be used before the user can change it again.

- Not display or allow printing of passwords on the screen while being entered
- Encrypt and store password files separately from systems data
- Lock, disable or delete vendor accounts after project completion
- Not display system or application identifiers until the login process has been completed
- Passwords shall be masked and not displayed as plain-text when they are entered by a user.
- Not provide help messages during the login process that would aid an unauthorized user
- Password of service account will be managed by MOHAP System administrators and will not be shared with any other team or vendor.

5. Password Communication

- Passwords shall not be revealed in conversations, inserted into email messages or any other forms of electronic or verbal communication.
- Passwords shall not be written down, stored on any information system or storage device.
- Initial passwords shall only be valid for the first log-on attempt within a period of 48 hours from the time the password is handed over. Users shall be forced to change the password on first use.
- In case of forgotten passwords, temporary passwords shall be issued only after positive identification of the user.

6. Password History Policy

- User accounts that have system-level privileges granted through group memberships or programs shall have a unique password from all other accounts held by that user.
- Passwords shall be checked to ensure that they are not identical to any of the previous 3 passwords for the same account.

7. User Account Lock-Out Policy

- Information systems shall be configured to lock the User-ID to the information system where an incorrect user password has been used 5 times in sequence.
- If the account was locked out due to multiple invalid/incorrect password attempt; the account will be auto unlocked after 30 minutes.
- Locked user accounts shall be reactivated by IT Service Team in accordance with the formal procedures developed and implemented to reactivate user accounts. These procedures shall require identification of the user and determination of the reason for the lockout before re-instating the user account and providing a new user password.

8. Password Composition

All user-level and system-level passwords shall conform to the guidelines described below:

- Passwords shall contain at least one upper and one lower case and one number characters (e.g., a-z, A-Z).

- Passwords shall have numbers, special characters and letters e.g. 0-9, !@#$%^and*()_+|~-=\`{}[]:";'<>?,./).
- The password cannot be the same as the ID and cannot repeat the same number or letter (whether upper case or lower case) more than two times consecutively.

9. Password Reset

- New joiner
  Post new user account creation, the first login password should be a random password, which is communicated to the user via SMS service and this would be a onetime password, post login user will be forced to change the password.

- Existing User
  If any user forgets his / her password to the system, IT Service Desk will ask security question for validation (at least 3 attributes for example Bayanati number, line manager name, date of birth etc.) and post verification SMS service would be used to share the password with the user.

9.8.3 Asset Management Methodology

1. Introduction

The IT department of Ministry of Health and Prevention (MOHAP) provides IT services to all other business units of MOHAP and to other entities. Such services are provided with information assets which are crucial for the IT operations. The effective implementation of Information Security and IT Service Management systems requires that details of all the assets are recorded and updated regularly.

2. Purpose

This document defines the methodology for identification, valuation, classification, labelling and handling information assets, with a view to ensuring that appropriate level of protection is applied throughout the lifecycle of the information assets.

3. Applicability

This document is applicable to the IT services covered by the scope of Information Security and IT Service Management Systems as defined in ISMS Scope document and ITSM Scope document.

4. Information Asset Management (IAM) Overview

IAM is a continuous process that aims to identify and classify information assets to ensure that information, especially business-critical information, is appropriately handled and protected against threats that can negatively impact the information asset's confidentiality, integrity and eventually the business.

5. Key Definitions

Information Asset	A body of information that the organization must have to conduct its business operations.
Business Applications	Application programs that automate the business processes and contain the information assets.
Software Asset	Underlying infrastructure of the application, which includes operating systems, databases, and applications.
Hardware Asset	Tangible assets of the organization, such as Servers, Network Devices and Peripherals.
Information Asset Owner	Individual responsible for determining the value, sensitivity level, methods to protect the information asset and to do a periodic review of the same.
Information Custodian	Person responsible for overseeing and implementing the necessary safeguards to protect the information assets, at the level classified by the Information Owner.
Information Asset Type	Information assets are categorized into following types: ▪ Primary Asset: • Information

	• People • Process ▪ Supporting/ Underlying Asset • Hardware • Software • Business Application The asset type will define the approach to undertake the classification and valuation processes.
Information Asset Classification	Classification of assets into classes based on common characteristics, andwhich need common protection levels to secure the information's confidentiality, integrity and availability. The information asset. classification represents the sensitivity level of the information asset.
Confidentiality	One of the information security pillars that set the requirements forensuring that information is not disclosed to unauthorized parties.
Integrity	Sets the requirements for ensuring that the data and information is notmodified maliciously or accidentally.
Availability	Sets the requirements for ensuring that the data and information isavailable and accessible to the users when required.

6. Information Asset Identification, Recording and Valuation

6.1 Asset Identification

The information assets of the organization are identified by the asset owners, who may be from the IT department and the business units.

6.2 Asset Recording

The details of the information assets shall be recorded in an Asset Register. The Asset Register should contain the following details:

- Asset Identification No.
- Asset Name
- Related application
- Asset owner
- Asset custodian
- Asset location
- Asset type

6.3 Asset Valuation

The value of the information assets is determined using a qualitative method. The importance of the asset is represented considering the requirements of confidentiality, integrity and availability.

- **Confidentiality** ensures that the information is only accessible to authorized parties. The confidentiality value describes the importance of keeping the asset confidential.

- **Integrity** ensures that the information is not changed. The integrity value describes the importance of sustaining the asset and protecting it from unauthorized changes.
- **Availability** ensures that the asset be accessible to the users when required. The availability value describes the importance of an asset being available.

Valuation	Valuation Scale	Confidentiality	Integrity	Availability
1	Low	Open for all (texton the public website, brochures) Classification: Public	No direct business impact if integrity is compromised. (e.g. internal phone directory, location maps, help files)	No impact to businessif the information is unavailable. (e.g. internal phone directory, location maps, help files not available for more than one day)
2	Medium	Internal employee usage only (internal phone directory, policy documents, work procedures) Classification: Internal	Minor business impact if integrity is compromised (e.g. information on the web site, internal procedures)	Minor impact to business if information is unavailable. (e.g. information on intranet not availablefor more than 12 hours up to 24 hours)
3	High	Restricted access on a need to know basis only (e.g. informationfrom other entities, contracts, financial information) Classification: Restricted	Noticeable business impact and disruption of the work process if integrity is compromised (e.g. research information, information received from other entities)	High impact to business if information is unavailable (e.g. Business Strategy not available for morethan 4 hours up to 12 hours)
4	Very High	Restricted to an exclusive few only (e.g., VIP visit details, new project plans) Classification: Confidential	Serious business impact if integrity is compromised (e.g. Business Strategy plans, Financial records etc.)	Business cannot operate at all if information is unavailable. (e.g. Business Continuity plans not available for more than 1 hour)

Business Impact = Sum Of (Value for Confidentiality + Value for Integrity + Value for Availability)

Business Impact is used for assessing the risk in respect of each asset.

7. Information Asset Classification

The objective of information classification is to determine the sensitivity level of the information asset.

The classification level mentioned under column “Confidentiality” as part of Asset Valuation shall be as the Asset classification value.

This Asset classification is used for determining the controls required in respect of information contained in the assets and the handling of such information – the transfer, copying, retention and deletion of information.

The Asset classification value shall be recorded in the Asset Register.

8. Information Asset Labelling and Handling

8.1 Asset labelling

All physical information assets shall be labelled, i.e. marked with the unique asset inventory number.

8.2 Information Asset Handling

Each information asset class requires specific requirements for handling the information in its various forms.

The guidelines for handling are given below;

Area	Public	Internal	Restricted	Confidential
Electronic Storage Location	No restrictions.	All except external Web and external FTP	Managed and monitored servers	Company desktop/laptop, corporate file share or corporate database
Electronic Storage Protection	Unprotected. Encryption not necessary	Optional Password authentication. Internal laptops/desktops: Encryption advised Removable media: Encryption advised	Validated strong passwords and / or multifactor authentication. Internal laptops/desktops: Encryption mandated Removable media: Encryption mandated	Validated strong passwords or multifactor authentication. Removable media: Encrypted Isolated laptops secured, encrypted, hardened, without network connectivity, USB ports and printing disabled,

				stored in secure vaults when not in use
Physical Storage Protection	No restrictions.	Take reasonable precautions to restrict access.	Store in a locked container. Restrict access to authorized people.	Store in a locked container. Restrict access to authorized people.
Granting of Access	No restrictions on read. Update rights to Information owner or designate	Read: Information owner designates by role. Update: Information owner designates by role.	Read: Information owner designates by individual. Update: Information owner designates by individual.	Read: Information owner designates by individual. Update: Information owner designates by individual.
Electronic Transmission	No restrictions. Information can be transferred freely	Secure file sharing methods advised such as password protected files Encrypted USBs advised	Encrypted. Secure file sharing mandated Encrypted USBs mandated	Only by information owner, with encryption. Should be sent only with password protection Should be transferred only to secure isolated laptops
Fax	No restrictions.	Reasonable precautions to restrict access and confirm delivery to recipient.	Restrict access to the sending machine during transmission and notify the recipient to stand by for receipt of fax and delivery confirmation. Password protected recipient mailbox or attended receipt	Restrict access to the sending machine during transmission and notify the recipient to stand by for receipt of fax and delivery confirmation. Password protected recipient mailbox or attended receipt

Copying	No restrictions.	In-house copying preferred. Shred or place spoils and overruns in secure bins. If outside copying is used, then the original should be returned to the company, and spoils should be destroyed by the supplier.	Only In-house copying. Shred spoils or overruns.	Only In-house copying. Shred spoils or overruns.
Destruction	Any.	Shred or place in secure bins	Shred.	Shred.
Labeling	Must be explicitly labeled or defined as "public" in "Company Information Classifications."	All unlabeled information should be considered internal unless otherwise labeled or defined.	Label all electronic (e.g., Word, Excel, PowerPoint) and physical documents. Recommend use of watermark option, where possible, in electronic documents.	Label all electronic (e.g., Word, Excel, PowerPoint) and physical documents. Use watermark option where possible in electronic documents.
Release electronically to third parties	No restriction	After signing of Non-disclosure agreement	Owner approval required and signing non-disclosure agreement Secure file sharing methods with restricted access to be used	Should not be shared

9.8.4 Internet and Email Policy

1. Introduction

The IT department of Ministry of Health and Prevention (MOHAP) provides IT services to all other business units of MOHAP and to other entities. Such services are provided with information assets which are crucial for the IT operations. The effective implementation of Information Security requires that risks to the processes, operations and assets are identified, analyzed, and mitigated.

2. Purpose

To regulate appropriate usage of Internet and Email for legitimate business purposes and protect MOHAP information assets from related threats and risks.

3. Scope

This policy applies to all users of MOHAP's Information Systems Assets, including but not limited to all MOHAP Employees, Employees of temporary employment agencies, Vendors, Business Partners, and Agents working on behalf of MOHAP.

4. Internet Policy Statements

4.1 Access to internet will be based on business requirements and specific job responsibilities of the individuals within MOHAP.
4.2 All requests for internet access shall be routed through the IT Manager at each location.
4.3 Internet user account creation shall be provided upon approval from PMO.
4.4 There shall be four groups of users for internet access, viz. Users Group, Managers Group, VIP Group and No-access Group.

- All the managers of IT shall be part of the Managers Group
- All the Directors shall form the VIP Group

4.5 Any exceptions to the policy shall be approved by PMO / IT representative at the individual locations.
4.6 All user accounts provisioned with internet access shall adhere to MOHAP Password policy.
4.7 Users shall not download and install any software / application / utility from the internet. If a user needs such application / utility for business requirements, a request shall be raised to IT Help Desk.
4.8 All Users shall connect to the internet only through the MOHAP Web Proxy.
4.9 The MOHAP Web Proxy shall log all user activities.
4.10 The MOHAP Web Proxy shall not cache user information and cryptographic material.
4.11 The MOHAP Web Proxy shall have separate network interface for Outside, Internal and Management connections.
4.12 The MOHAP Web Proxy shall have only the required TCP/UDP ports enabled in line with the business requirements.

5. Email Policy Statements

5.1. All emails entering/exiting the network shall pass through the SMTP Gateway Filter. This filter device has the capability to scan the email for;

- Virus, spyware, malware content
- Spam content
- Any specific configured rule base scanning

5.2. Any such email is blocked at the gateway level itself and is not allowed to enter the organizational network.

5.3. Anti-Phishing service shall be implemented to proactively identify phishing emails (by planting probes on the Internet) and illegitimate use of corporate logos in emails etc. Actions will be initiated to minimize the impact of any phishing email and to educate the users of such phishing emails.

9.8.5 Encryption and Key Management Policy

1. Introduction

The IT&HIS department of Ministry of Health and Prevention (MOHAP) provides IT services to all other business units of MOHAP and to other entities. Such services are provided with information assets which are crucial for the IT operations. The effective implementation of Information Security and IT Service Management systems requires that the systems have security controls for encryption.

2. Purpose

To ensure that encryption keys are secured and managed throughout the life cycle.

3. Scope

- This policy covers the systems and networks covered by the scope of Information Security Management System as described in “ISMS Scope”.
- Usage of encryption includes: windows logon, remote access, sensitive data encryption, emails, document encryption, application single sign-on, and web application logon.

4. Policy Statements

A. General

- Proven, standard algorithms such as AES and RSA should be used as the basis for encryption technologies.
- All transmissions of sensitive data (including but not limited to, identification & authentication) over the Internet shall use encryption.
- Sensitive / confidential data stored on portable / removable media (such as laptops) shall be encrypted.
- Data backup storage shall be encrypted.
- All cryptographic keys shall be protected against unauthorized access.

B. Key Size & Algorithm

- Cryptographic key lengths shall be at least 128 bits; however recommended key strength should be 256-bits.
- Encryption key length requirements shall be reviewed annually and upgraded as technology allows.

C. Administration & Key Management

- IT shall manage all encryption keys.
- Web servers with SSLv3/ TLSv1.3 in strong encryption mode shall be used to secure sensitive data for publicly accessed services over the Internet.
- Cryptographic techniques shall be periodically re-assessed for their continued effectiveness.
- Encryption keys shall be securely distributed.
- Keys in storage and transit shall be encrypted.
- The administrator should store encryption keys in a secured manner inside a safe at both main and backup computer sites.

9.8.6 Network Security Policy

1. Introduction

The IT&HIS department of Ministry of Health and Prevention (MOHAP) provides IT services to all other business units of MOHAP and to other entities. Such services are provided with information assets which are crucial for the IT operations. The effective implementation of Information Security and IT Service Management systems requires that the systems have security controls to keep the network secured.

2. Purpose

The purpose of this policy is to establish security requirements for managing the MOHAP's internal and external network for appropriate and secure operations of the information processing facilities and protect the confidentiality, integrity and availability of data flowing through MOHAP's networks.

3. Scope

The scope of this policy covers all network communication, and, information systems and environments managed by MOHAP.

4. Policy Details

A. Network Security Policy

Access to the information resources of MOHAP will be based on business requirements and specific job responsibilities of the individuals accessing the system and maintaining the infrastructure, software and hardware.

B. Baseline Network Security

- All Network administrative accounts shall adhere to the MOHAP Password policy.
- All MOHAP DMZs shall be configured at layer 2 and routing shall not be used.
- Changes to the DMZs shall be subject to the MOHAP Change Management processes and should adhere to relevant MOHAP security standards and policies.
- Appropriate VLANs should be created based on criticality and sensitivity of the systems to be hosted.
- VLANs shall not be shared between different services and systems.
- Only RFC1918 addresses shall be used on the network.
- All systems and services shall have a network design associated to them, which shows IP addresses, gateways etc including clear marking of data flows.
- Core switches shall use layer 3 routing.
- Network infrastructure shall be monitored by a network / systems management tool.
- DMZ gateways shall be adequately controlled through deployment of appropriate security devices.
- DHCP shall not be enabled for business-critical servers.
- All Network infrastructures shall be backed up to a centralized management server.
- Servers performing management functions shall be located within a centralized single management network.

- Redundancy shall be built into the network infrastructure.
- IP addressing and sub-netting shall show distinction between the different support teams, users and locations.
- Packet sniffing, Packet capturing or any invasive technique that enables client data to be captured shall be approved by security and the relevant Data and System Owners beforehand.
- All network infrastructures shall use a centralized time source.
- Detailed Layer 3 Network Diagrams for the internal network shall be maintained and updated (when required) by MOHAP Network team.

C. Network Segregation

- There shall be physical and logical separation between the development, test/ staging and production network.
- Pilot system installations shall be kept on a separate network. This network shall not have any connectivity to the development, test / staging or production network.
- Connections shall not be permitted between the test/development and the production/live network.
- Network / System hardware other than approved security devices shall not be shared between test / development and production/live network.
- No paths other than agreed security devices shall exist between test/development and the production/live network.
- All changes shall be performed, checked, tested and approved in the test/development environment before being released into production / live network.
- IP addressing of the test/development network shall be different to production/live network, with the address space being horizontally scalable.
- Network Segregation and related access control policies shall be reviewed and updated periodically based on new business requirements.

D. Third Party Access

- Access to MOHAP Hardware and software for vendors should be approved by the management.
- VPN access to vendors should be given on demand only after approval from MOHAP project manager. Account validity should be based on required task duration.
- Vendor accounts will be clearly marked in Windows AD to indicate the actual end-user name and contact number. Contact details will be used in case of any security or operations need or emergency.
- Vendor VPN account shall be protected by MFA (Multifactor authentication) to avoid any security breach.
- It is the responsibility of the Application and IT Infrastructure team to supervise the access provided to their respective vendors. They should ensure to raise an access revoke request as soon as the vendor contract is over/terminated.
- In addition to VPN; as and when needed WebEx sessions can be used to get vendor support on any server. The session shall be fully supervised by a privileged user from MOHAP Side (System Admin or Application Admin)

- Password of service account will be managed by MOHAP System administrators and will not be shared with any other team or vendor.

E. Network Infrastructure

- Standardized builds, where possible shall be used for Network devices.
- Manual and build instructions shall be created, used and updated for network devices.
- ACLs shall be used on all switches and routers.
- Switches shall not be shared between systems and services of different protective markings (classification levels).
- Anti-spoofing shall be enabled on all firewalls.
- Firewalls shall be capable of stateful inspection.
- All critical network and security shall be deployed in a high availability mode.
- Network Infrastructure shall be patched to the latest tested patch level.
- Default accounts shall follow the guidelines defined within the MOHAP Access Control policy.
- Centralized logging shall be enabled for all network infrastructure components supporting production systems.
- Management ports shall not be accessible to anyone other than the MOHAP Network team that support and maintain the devices.
- Network admission controls shall be enabled on network from where sensitive systems are accessed.
- Network infrastructure supporting access to sensitive production systems shall be restricted only to authorized users allowed to access and manage those systems.
- MOHAP staff personal laptops and desktops shall not be connected to MOHAP internal network.
- ADSL connections for internet connectivity shall not be permitted for the users.

F. Operational Procedures

- Secure protocols shall be used to manage network devices.
- An explicit drop rules shall be defined in all Firewall rule bases and ACLs. This shall specify Any Source to Any Destination, using Any Port and be positioned at the bottom of the rule bases.
- Explicit drop rules shall be used throughout the rule base; they shall not replace the explicit drop at the bottom of the rule base.
- A stealth rule shall be created at the top of the rule base.
- All objects created within the rule base shall follow a standardized naming convention.
- All firewall rules shall be treated as uni-directional unless proved otherwise.
- Any firewall rule that needs to be bi-directional shall be approved by the Security team before being allowed.
- Large port ranges shall not be used unless absolutely necessary and other attempts to limit the range have been exhausted.
- Network Infrastructure shall be patched to the latest tested patch level.
- MOHAP Network operations team shall limit network devices to activating only those ports, protocols and services required to support agreed information services. Unnecessary capabilities of the network device shall not be enabled

- Ingress, Egress filtering and Unicast Reverse Path Forwarding shall be deployed on MOHAP gateway devices to limit the potential for IP address spoofing.

G. Change Management Procedures

- All network Changes shall go through the formal change management process and be approved before implementation.
- Emergency network changes shall retrospectively go through the change management process.
- All network changes shall be performed, checked, tested and approved in the test/development environment before being released into live.
- The change management process shall not be used as the vehicle for acceptance of new services into the live/production network.

H. Network Risk assessment

- Risk assessment on individual network components and the network as a whole shall be performed to identify vulnerabilities
- Specific network controls needed to mitigate the vulnerabilities identified shall be implemented
- Automated scans of network ports shall be conducted by the Entity's Information Security personnel or approved third party and compared to a known, agreed configuration baseline. If a new port is found open an alert shall be generated.

9.8.7 Secure Development Policy

1. Introduction

The IT&HIS department of Ministry of Health and Prevention (MOHAP) provides IT services to all other business units of MOHAP and to other entities. Such services are provided with information assets which are crucial for the IT operations. The effective implementation of Information Security and IT Service Management systems requires that details of the secure development controls are implemented and checked regularly.

2. Purpose

The purpose of this policy is to define the policy related to secure software development and maintenance. It is a well-accepted principle that security should be considered at the design stage of the application or service and not at the delivery stage as an after-thought.

3. Scope

This policy is applicable to all security assessments conducted on MOHAP technology infrastructure, applications, networks and physical security components collectively referred to as 'computer systems'.

4. Secure System Engineering

- The information security controls shall be applied to all new in-house or third-party developed MOHAP applications and services. Information Security shall be involved in the project team with the role and responsibility of conducting a risk assessment of the service/application to MOHAP information and IT infrastructure.
- New technologies should be analyzed for security risks / vulnerabilities prior to being implemented / installed with the development architecture.
- All ready to use "off the shelf" software applications should be evaluated for required security controls prior to finalizing any application for use.
- Development environment shall be managed by source safe utility with complete history and version track.
- Developers shall log in using individual credentials.
- Support team shall have view-only access on production to verify the issues and support accordingly.

5. Secure System Development

5.1. Training shall be provided as part of new implementation or enhancement of the existing system

5.2. New implementation of systems or applications shall include the following:

- Roles and responsibilities for design, development and implementation
- Segregation of development, test and production environments
- In those cases where staging environment is not available due to license issues, development environment may be used for testing purpose.
- Production team shall not have development tools and no access for developers. All packages shall be deployed by concerned people with corresponding access.

- Sensitivity of data processed, such as Driving License Number, Emirates ID number, Credit card details, if any, etc.
- Compliance to best practices related to development and coding, such as OWASP
- Approvals for development, testing and movement to production
- Post implementation review and support
- Training material along with BRD shall be prepared by analysis team whereas FSD shall be prepared by the technical team.
- Training for internal staff shall be conducted by support team
- All bugs, issues and errors shall be solved using case management system where case reference shall be added using admin logon along with history log to track all changes.

6. Project Management

6.1 Security requirements should be identified at the requirements phase of a project and justified, agreed and documented as part of the overall business case for any new information system, or enhancements to existing systems under the development to mitigate the risk resulting from loss, misuse, or unauthorized access to or modification of the information therein.

6.2 Project schedule and plan shall be developed using Microsoft Project.

7. Outsourced Development

If and when software development is outsourced, the following measures shall be considered by the Development team and the Information Security Manager, to ensure that information security requirements are not compromised:

- Licensing agreements and intellectual property rights
- Certification of quality of the development process
- Escrow arrangements with the developers
- Rights of access for auditing quality and accuracy of development
- Compliance to development and coding best practices
- Training and Knowledge transfer
- Security testing to detect Trojan codes
- Compliance with legal and regulatory requirements

8. System Security Testing

8.1. Testing of new systems / applications shall include the following:

- Design and definition of security requirements by the business owners
- Acceptance criteria for systems considering security requirements
- c. Sign-off from the project owners before presenting for User Acceptance Test.

8.2. System testing should be performed in the testing environment.

8.3. Access control should be implemented to ensure that developers, testers and operational staff have access only to Development, Testing and Production systems, respectively.

8.4. An audit log must be maintained for all access to testing environment

8.5. Dummy test data shall be used / be generated for testing purpose and actual operational information should not be used.

9.8.8 Backup and Restore policy

1. Introduction

The IT&HIS department of Ministry of Health and Prevention (MOHAP) provides IT services to all other business units of MOHAP and to other entities. Such services are provided with information assets which are crucial for the IT operations. The effective implementation of Information Security and IT Service Management systems requires that details of all the critical information are well backed up and restored regularly.

2. Purpose

The purpose of this policy is to ensure that information systems and business applications are protected and recoverable in case of data corruption or system failure.

3. Definitions

- **Business Application:** Software program that helps a business increase productivity. The software program can be used for internal business processes like HR, finance, purchasing, or external business services, like billing and call center.
- **Information System:** Data records and activities that process the data and information in an organization and include the organization's manual and automated processes.
- **Business Information:** Soft copy of documents, reports, customer and staff records, system configurations, databases, files that are used for business purposes.
- **Backup:** Saving copy of data on storage media.
- **Archive:** Saving old or unused data onto storage media for the purpose of releasing online storage.
- **Restore:** Process of copying offline data that are saved on backup media to online storage.

4. Scope

This policy applies to all systems, devices and applications used for business operations.

5. Policy Details

A. Backup Policy for KDC Virtual Machines

Frequency	Backup Storage Duration
Daly Incremental	2 Weeks
Weekly Full	1 Month
Monthly Full	1 Week and 6 Months on Tapes

- The Daily Incremental Backups will be stored on Disk Appliance for a period of 2 Weeks.

- The Weekly Full Backups will be stored on Disk Appliance for a period of 1 months.
- **(Full Backup is scheduled on Every Thursday, Friday and Saturday)**
- The Monthly Backups will be stored on Disk Appliance for a period of 1 Weeks and then the Backup will be stored on Tape for 6 Months - **Full backup scheduled last day of the every month.**
- Any on demand backups of VM's will be stored on Tapes for 6 Months on request basis.
- Backups in our environment are scheduled to run over the night.
- All kind of restoration / Backup on demand can be done in the day time.
- Backups are getting started from 3 PM onwards continuously to run over the night.
- No restorations can be performed between 3 PM to 7 AM which will impact the backups.
- **Tape Rotation** - Monthly Backups on Tapes from KDC to MOHAP HQ

B. Backup Policy for Hospitals Virtual Machines

Frequency	Backup Storage Duration
Daly Incremental	2 Weeks
Weekly Full	1 Month
Monthly Full	2 Week and 6 Months on Tapes

- The Daily Incremental Backups will be stored on Disk Appliance for a period of 2 Weeks.
- The Weekly Full Backups will be stored on Disk Appliance for a period of 1 months.
  (Full Backup is scheduled on Every Thursday, Friday and Saturday)
- The Monthly Backups will be stored on Disk Appliance for a period of 2 Weeks and then the Backup will be stored on Tape for 6 Months - **Full backup scheduled last day of the every month.**
- Any on demand backups of VM's will be stored on Tapes for 6 Months on request basis.
- Backups in our environment are scheduled to run over night.
- All kind of restoration / Backup on demand can be done in the day time.
- Backups are getting started from 10 PM onwards continuously to run over the night.
- No restorations can be performed between 10 PM to 7 AM which will impact the backups.
- **Tape Rotation** – Monthly Backups on Tapes from Hospital to MOHAP HQ

C. Exchange 2010 and 2016 Emails

Frequency	Backup Storage Duration
Daily Incremental (Backups Schedule Every 6 Hours)	1 Month
Weekly Full	1 Month
Monthly Full	1 Week and 6 Months on Tapes

- The Daily Incremental Backups will be stored on Disk Appliance for a period of 1 Month.
- The Weekly Full Backups will be stored on Disk Appliance for a period of 1 months.
- (**Full backup scheduled on every Friday 12:30 AM**)
- The Monthly Backups will be stored on Disk Appliance for a period of 1 Weeks and then the Backup will be stored on Tape for 6 Months - **Full backup scheduled last day of the every month**.
- Any on demand backups of Emails will be stored on Tapes for 6 Months on request basis.
- Backups in our environment are scheduled to run over night.
- All kind of restoration / Backup on demand can be done in the day time.
- Backups are getting started from 3 PM onwards continuously to run over the night.
- No restorations can be performed between 3 PM to 7 AM which will impact the backups.
- **Tape Rotation** - Monthly Backups on Tapes from KDC to MOHAP HQ

D. SQL Data Base

Frequency	Backup Storage Duration
Daily Incremental	2 Weeks
Daily Transaction Logs	1 Month
Weekly Full	1 Month
Monthly Full	1 Week and 6 Months on Tapes

- The Daily Incremental Backups will be stored on Disk Appliance for a period of 2 Weeks.
- The Daily Transaction Logs will be Stored on Disk Appliance for a period of 1 Month

- The Weekly Full Backups will be stored on Disk Appliance for a period of 1 months.
- (**Full Backup is scheduled on Every Thursday, Friday and Saturday**)
- The Monthly Backups will be stored on Disk Appliance for a period of 1 Weeks and then the Backup will be stored on Tape from 6 Months - **Full backup scheduled last day of the every month**.
- Any on demand backups of Database will be stored on Tapes for 6 Months on request basis.
- Backups in our environment are scheduled to run over night.
- All kind of restoration / Backup on demand can be done in the day time.
- Backups are getting started from 3 PM onwards continuously to run over the night.
- No restorations can be performed between 3 PM to 7 AM which will impact the backups.
- **Tape Rotation** - Monthly Backups on Tapes from KDC to MOHAP HQ

E. Oracle Data Base

Frequency	Backup Storage Duration
Daly Incremental	2 Weeks
Daily Transaction Logs	1 Month
Weekly Full	1 Month
Monthly Full	1 Week and 6 Months on Tapes

- The Daily Incremental Backups will be stored on Disk Appliance for a period of 2 Weeks.
- The Daily Archive Logs will be Stored on Disk Appliance for a period of 1 Month
- The Weekly Full Backups will be stored on Disk Appliance for a period of 1 months.
- (**Full Backup is scheduled on Every Thursday, Friday and Saturday**)
- The Monthly Backups will be stored on Disk Appliance for a period of 1 Weeks and then the Backup will be stored on Tape from 6 Months - **Full backup scheduled last day of the every month**.
- Any on demand backups of Database will be stored on Tapes for 6 Months on request basis.
- Backups in our environment are scheduled to run over night.
- All kind of restoration / Backup on demand can be done in the day time.
- Backups are getting started from 3 PM onwards continuously to run over the night.
- No restorations can be performed between 3 PM to 7 AM which will impact the backups.
- **Tape Rotation** - Monthly Backups on Tapes from KDC to MOHAP HQ.

Medical Districts and Development Backups Policy need to update once Backup Setup is configured.

9.8.9 Risk Management Methodology

1. Introduction

The IT&HIS department of Ministry of Health and Prevention (MOHAP) provides IT services to all other business units of MOHAP and to other entities. Such services are provided with information assets which are crucial for the IT operations. The effective implementation of Information Security requires that risks to the processes, operations and assets are identified, analysed, and mitigated.

2. Purpose

This document defines the Risk Management Methodology for IT&HIS Department with a view to ensuring that risks to business operations are mitigated to the extent possible.

3. Applicability

This document is applicable to the IT services covered by the scope of Information Security Management System as defined in ISMS Scope document.

4. Key responsibilities

Risk Management is a joint responsibility of senior management, IT management, information security management and the business application / service owners. An overview of the key roles involved in the methodology is given below.

Information Security Steering Committee (ISSC)

- Oversee the management and implementation of the Risk Management process;
- Review and approve information security risk assessment, risk treatment plan and residual risks.

Chief Information Security Officer

- Coordinate with various departments/ risk owners to conduct periodic risk assessments based on a schedule or as per organizational requirements; and
- Create awareness among employees to effectively contribute to the IRM process.

Information Risk Owners

- Ensure sufficient and effective controls are in place to address the risks they own;
- Identify risks related to their area of operation, evaluate controls available and their effectiveness, identify controls where necessary and accept the residual risks;
- Engage Information Security team to help develop risk mitigation controls for identified risks.

5. Key Definitions

Information Asset	A body of information that the organization must have to conduct its business operations. Information assets include hardware, software, application, people, document and information in electronic form

Threat	A potential event that can compromise the Confidentiality, Integrity and Availability (CIA) of information.
Vulnerability	A weakness in the design, implementation or operations that could be exploited to violate or bypass existing security control that may result in the exposure of CIA of information assets
Risk	Adverse impact caused by a risk occurrence. The risk occurs when a threat exploits a vulnerability of an information asset.
Risk Management	Continuous process of risk identification, assessment, mitigation, treatment and monitoring
Risk register	A repository for all the risks identified and for each risk, the impact, probability and mitigation measures
Risk Owner	Individual responsible for managing the risk, risk evaluation and selection of the risk mitigating option
Control	Countermeasure or safeguard such as a procedure or action that mitigates a risk
Inherent Risk	The risk level without considering the implemented controls
Residual Risk	The remaining risk after considering the effectiveness of current controls
Risk Treatment	The process of implementing the risk reduction options that comprises a list of the selected controls
Risk Acceptance	A risk mitigation option where the decision is made to accept the Residual risk without the addition of further controls

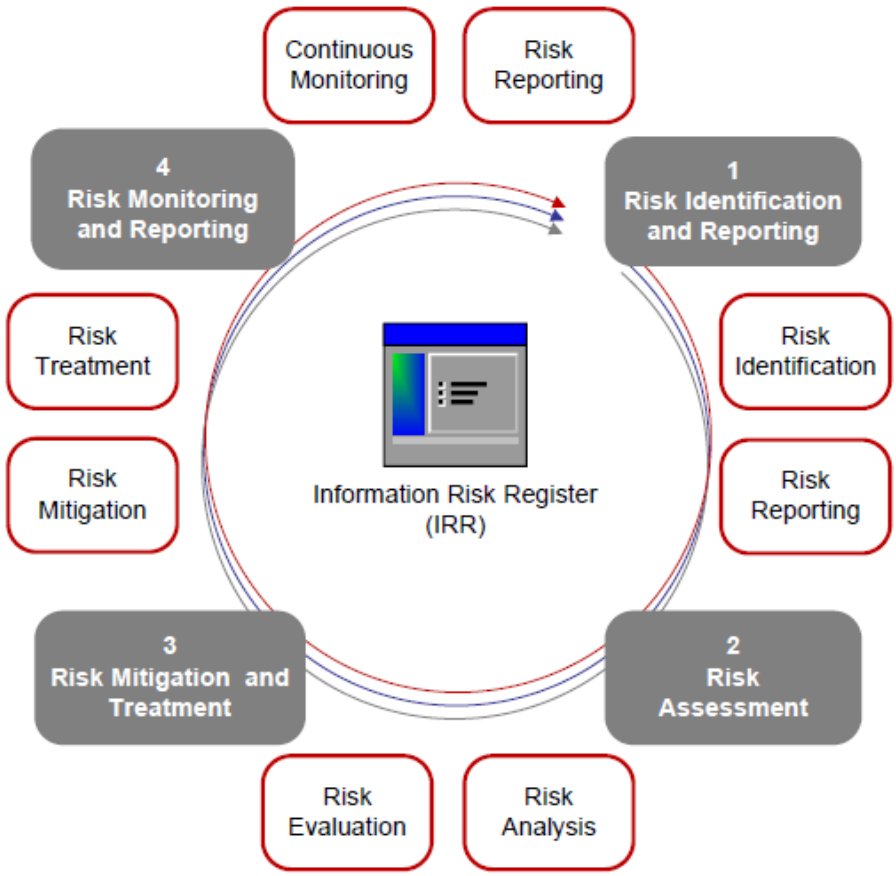
Risk Avoidance	A risk mitigation option where the decision is made to withdraw from or not become involved in the risk circumstance and situation
Risk Transfer:	A risk mitigation option where the decision is made to share the burden of loss in the event of a risk occurrence with another party
Risk Monitoring	The process of monitoring the implementation of the risk treatment plan and triggering risk reassessments as required

6. Alignment to best practices

The techniques used in this IRM methodology are inferred from leading practices such as ISO 27005, ISO 31000, OCTAVE, etc. However, the methodology is customized to suit the specific requirements of the organization.

7. Risk Management workflow

Risk Management is a continuous cycle to minimize the negative impact of risks to the business operations.



8. Risk Management process

a. Threats and Vulnerabilities

Threats and vulnerabilities are inputs to the risk management processes. These may include threats that have occurred or are likely to occur in future. Threats may be identified by analysing incidents, help desk logs, and security logs, reviewing of public documentation on existing vulnerabilities in commercially published systems, external factors such as new legislations and regulations, and by talking to individual users, service / process owners.

The Risk register shall contain a comprehensive list of threats and vulnerabilities, which shall be updated as and when a new threat or vulnerability is identified.

b. Threat-Vulnerability Pair

A vulnerability may exploit a corresponding threat. A pair of a threat and its related vulnerability (a T-V pair) constitutes a possible risk.

c. Risk identification

Risk identification may be triggered at any level based on a defined schedule:

- Introduction of major changes to the existing systems or applications or during acquisition of new systems;
- Incidents reported that may result or indicate potential information risk exposure;
- IT-Security and Information Security Audit reports;
- Internal and External Vulnerability Assessment;
- Operational reports generated by the departments;
- Error reports and Service Desk reports;
- Complaints from the end users or IT users; and
- Independent Security consultants and authentic public domain knowledge bases.
- A single asset may have multiple T-V pairs associated with it. Similarly, a single threat may have multiple vulnerabilities and vice-versa.

d. Risk Assessment

i. Risk Assessment Overview

The next step is to rate the evaluate the risks based on judgment and past experience (qualitative measure). Key attributes include:

- Risk Impact
- Likelihood
- Risk Value

ii. Risk Impact

The risks are rates based on their impact on business operations. A three-point scale is used to determine the impact rating.

Risk Impact	Assigned Value	Definition
High	3	T-V pair has a high impact, causing major damage
Medium	2	T-V pair has a normal impact, causing moderate damage
Low	1	T-V pair has a low impact, causing little damage

iii. Likelihood of Risk

Likelihood of the occurrence of risks is estimated based on experience, information from stakeholders, and reports of incidents.

Risk Likelihood	Assigned Value	Definition
Likely	3	There is a high chance of risk materializing
Less Likely	2	There is a moderate chance of risk materializing
Unlikely	1	There is a low chance of risk materializing

For each item of risk, the existing controls are identified. The impact and likelihood of occurrence are estimated after considering the controls implemented.

iv. Inherent Risk Value

The Inherent Risk Value is calculated as per formula below:

Inherent Risk = Asset Value * Impact Rating * Likelihood Rating

v. Inherent Risk Rating

The Inherent Risk Rating is obtained as per details below:

Risk Value	Risk Rating
Greater than 54	High
28 to 54	Medium
Less than 28	Low

e. Acceptable Level of Risk

Risks whose rating is 'Low' are Acceptable. Risk treatment options will be evaluated in respect of High and Medium rated risks.

f. Risk Mitigation

The objective of Risk Mitigation process is to reduce the risk rating by considering additional controls to be implemented.

i. Risk mitigation options

Any one of the following options may be selected:

1. Risk Avoidance – risk may be avoided by eliminating the possibility of the threat materializing
2. Risk reduction – additional controls may be implemented to lower the likelihood of the threat occurring
3. Risk transfer – risk may be transferred to a third party, such as insurance company
4. Risk acceptance – the risk may be accepted under the following circumstances:
   - when none of the above options are possible
   - when the cost of implementing a control is higher than the loss that may arise due to the risk
   - when the risk rating is Low

ii. Selection of controls

The selected mitigation option and additional controls shall be recorded in the Risk Register. For each of the additional control, responsibility shall be assigned and a Target date agreed upon with the responsible person.

g. Assessment of Residual Risk

i. Revised impact

The revised Risk impact is determined after considering the mitigation options selected. The impact is calculated on the same scale as High, Medium, or Low.

ii. Revised Likelihood

The revised Likelihood is determined considering the additional controls identified for implementation. This revised likelihood is also classified as High, Medium, or Low.

iii. Residual Risk Value

Residual risk is calculated considering the revised impact and revised likelihood.

Residual Risk = Asset Value * Revised Impact Rating * Revised Likelihood Rating

iv. Residual Risk Rating

The Residual Risk Rating is also obtained in the same way:

Risk Value	Risk Rating
Greater than 54	High
28 to 54	Medium
Less than 28	Low

h. Update of Risk Register

The information obtained during each of the above processes shall be updated in the Risk register:

i. Approval

Approval from the Risk owners shall be obtained for the following:

- Risk assessment, risk impact, risk likelihood
- Mitigation options
- Residual risk

9. Risk Monitoring, Review, Reporting

It is necessary to ensure that the risks continue to be mitigated and remain within acceptable level. To achieve this, the threats, vulnerabilities, and the impact and likelihood of risks shall be continuously monitored.

a. Continuous monitoring

Monitoring of risks may be triggered by any of the following:

- Change in existing controls
- Change IT / organization environment
- Change in services / operations
- Incidents reported

b. Review of Risk Assessment

The entire cycle of risk management shall be performed at least once in a year, to ensure that emerging risks are addressed and mitigated.

c. Risk Reporting

A Risk Assessment Report shall be placed before the Information Security Steering Committee at the end of each cycle of Risk Assessment. The risk report shall contain:

- Summary of top risks, actions to be taken against them and the target date for addressing them
- Progress in the implementation of controls identified during earlier risk assessments
- Exceptions and concerns, if any.

10. REFERENCES

Area	Reference Links
Data Governance	Definition https://www.techtarget.com/searchdatamanagement/definition/data-governance https://www.emids.com/wp-content/uploads/2018/06/emids_WP_DataGovernance_2015.pdf Benefits https://www.utopiainc.com/resources/blog/data-governance-benefits-for-today-and-the-long-term
Data Quality	Data Quality Dimensions https://www.collibra.com/us/en/blog/the-6-dimensions-of-data-quality Metadata Management https://www.ovaledge.com/blog/data-governance-metadata-management-better-together ISO Certification https://www.iso.org/obp/ui/#iso:std:iso:8000:-61:ed-1:v1:en
Data Security & Privacy	Data Security https://www.techtarget.com/searchsecurity/Data-security-guide-Everything-you-need-to-know Data Privacy https://www.imperva.com/learn/data-security/data-privacy/ CIA Triad https://www.varonis.com/blog/cia-triad Data Confidentiality https://www.egnyte.com/guides/life-sciences/data-confidentiality Data Availability - https://www.tibco.com/reference-center/what-is-data-availability#:~:text=Data%20availability%20is%20when%20an,with%2024%2F7%20data%20availability.