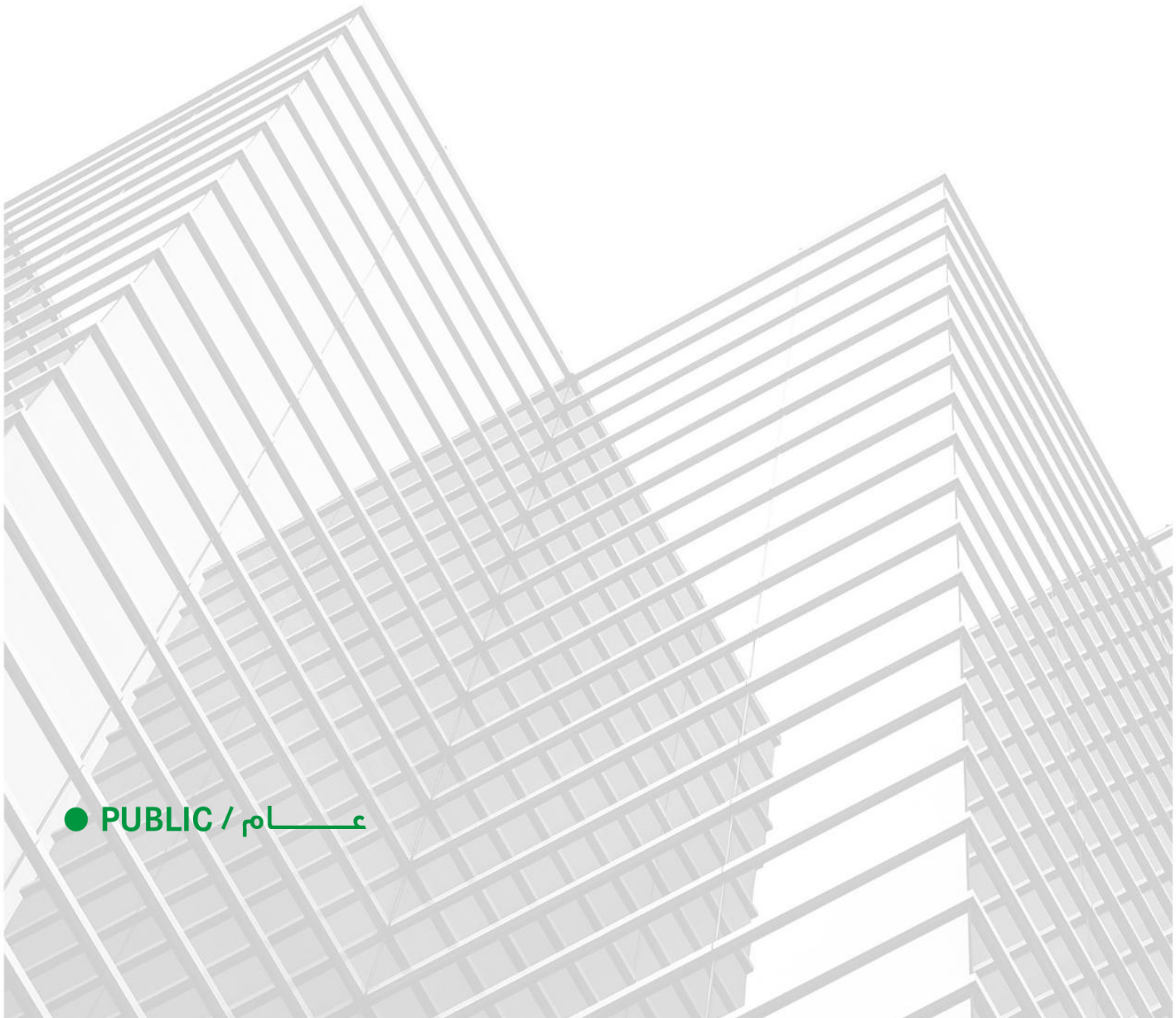
دائـــرة الـصـحـة
DEPARTMENT OF HEALTH

DATA SHARING, INTEGRATION & INTEROPERABILITY STANDARD



● PUBLIC / عـــــام

Document Ref. Number:	Data Sharing, Integration & Interoperability Standard		
New / Revised:	New	Version	V1
Publication Date:	December, 2025		
Effective Date:	April, 2026		
Document Control:	Strategic Affairs Sector		
Applies To:	All DoH Offices, Centers, Sectors & Organization Unit, Abu Dhabi Healthcare Ecosystem		
Owner:	Data and Digital Governance Office		
Revision Date:	December, 2028		
Revision Period:	Every three years or as and when needed		
Contact:	DDG@doh.gov.ae		

1.Standard Scope

1.1. The Department of Health (DoH) is committed to fostering seamless health information exchange across all affiliated entities and facilities within the Abu Dhabi Healthcare Ecosystem. This Data Sharing, Integration and Interoperability Standard governs the secure and efficient sharing of healthcare sector data between public and private healthcare entities, ensuring compliance with both national and international standards. This includes data sharing between DoH and other government entities, data sharing between healthcare entities, data sharing by entities to the Health Information Exchange Platform (Malaffi). The standard promotes data flow between departments and systems to enhance operational efficiency and support informed decision-making.

1.2. The scope of this standard includes the establishment of guidelines to maximize operational efficiency, reduce risk and enhance the value derived from data exchanges within the Abu Dhabi Healthcare Ecosystem. It mandates the adoption of national and international standards to ensure seamless integration and communication across diverse healthcare systems and platforms.

1.3. All data sharing activities must adhere to relevant data governance and security protocols. The implementation of this standard is expected to lead to significant improvements in health services, economic benefits, and enhanced patient safety through better frontline service delivery.

1.4. This standard applies to all entities within the Abu Dhabi Health Ecosystem, aiming for widespread adoption to foster a cohesive and interoperable healthcare environment that aligns with the strategic objectives of the DoH. This should be read in conjunction with the following guiding protocols – Data Sharing Request Protocol and Prepare Data for Sharing Protocol.

2. Definitions and Abbreviations

No.	Term / Abbreviation	Definition
2.1	Abu Dhabi Healthcare Ecosystem	Healthcare facilities, providers, insurance companies, pharmaceutical companies, health information exchange platforms, service providers, laboratories and research centers within Abu Dhabi's healthcare sector that generate, access, store, use, process and/or transmit health information.
2.2	Anonymized Data	Data that has gone through the process of protecting private or sensitive information by erasing or encrypting identifiers that connect an individual to stored data. The process cannot be reversed and there is no way to link this data to any individual.
2.3	Application Programming Interface (API)	A set of definitions of the ways one piece of computer software communicates with another. A web API allows computer programs to dynamically query a dataset using the World Wide Web. For example, a dataset showing the locations of hospitals and doctors surgeries may be made available for download as a single file (e.g. a CSV), or may be

		made available to developers through a Web API, such that a computer program could automatically retrieve a list of addresses for a particular area and display it on an online map alongside other relevant public and private sector digital data.
2.4	Data	A collection of information in a structured or unstructured form, such as numbers, characters, images, video, voice recordings, or symbols.
2.5	Data and Digital Governance Office (DDGO)	A centralized organizational unit responsible for overseeing the management, security, and ethical use of data and digital assets within an entity. The DDGO plays a strategic role in supporting data and digital strategies aimed at increasing the effectiveness of how the entity defines, stores, uses, and manages its data. This includes driving initiatives to enhance data governance practices, improve data quality, and ensure alignment with the organization's overall digital strategy.
2.6	Data Classification	The process of organizing and categorizing data based on its sensitivity, confidentiality, and criticality to an entity.
2.7	Data Custodian	The individual responsible to execute data-related initiatives and decisions associated with data management domains from a technical aspect. Serves as subject matter experts in information management, specializing in data systems/applications.
2.8	Data Exchange	Transfer of data between different organizations, systems, or applications. It's essentially the act of moving data from one place to another in a structured and secure way.
2.9	Data Integration Platform	A data integration layer that serves as a connection between various data sources and a target system, such as a data warehouse or another health application.
2.10	Data Interoperability	The ability of different information technology systems and software applications to access, exchange, integrate, and cooperatively use data in a coordinated manner, within and across organizational boundaries. It involves the seamless sharing of data among various systems, platforms, or components, ensuring that the data shared retains its meaning and does not lose its context or integrity.
2.11	Data Owner	The individual responsible for overseeing data management practices within a specific domain, ensuring compliance with data governance standards and regulations.
2.12	Data Sharing	The ability to distribute the same data resources to multiple users, applications or organizations through authorized channels while ensuring data consistency across all entities consuming the data.
2.13	Data Sharing Agreement (DSA)	Legal contract between two or more parties that outlines the rules and regulations for sharing specific data.
2.14	Data Sharing Request (DSR)	Formal request submitted by an individual, organization, or entity seeking access to specific datasets or information that is held by another party.
2.15	Data Steward	The individual responsible for managing and overseeing data usage and integrity within specific data domains, assisting Data Owners in resolving data-related issues.
2.16	Department of Health (DoH)	The regulatory authority responsible for overseeing healthcare operations within the Abu Dhabi healthcare ecosystem. The DoH aims to ensure high standards of healthcare delivery, public health initiatives, and patient safety, while promoting innovation and continuous improvement within the healthcare system.
2.17	DoH's Data and Digital Governance Office (DoH's DDGO)	An internal department within the DoH responsible for supporting and executing the data and digital governance strategy. The DDGO ensures compliance with data management and digital health policies, standards, guidelines, and frameworks across the healthcare ecosystem, while driving initiatives that enhance the effectiveness of how healthcare data is defined, stored, used, and managed to support the DoH's objectives.

2.18	External Data Sharing	The transfer or exchange of data between an organization and external parties, such as third parties, partners, or regulatory bodies, typically governed by data-sharing agreements and compliance standards.
2.19	Healthcare Interoperability Framework	Set of guidelines and resources that define how healthcare data should be exchanged seamlessly between different healthcare information systems.
2.20	Internal Data Sharing	The transfer or exchange of data between departments or entities within the same organization to support operations, decision-making, or collaboration.
2.21	Interoperability Standards	Common languages that different systems and devices use to communicate and exchange data seamlessly.
2.22	Metadata	Structured information that describes, explains, or provides context about a dataset, making it easier to find, manage, and utilize the data. It includes details such as the source, format, creation date, author, and relevant keywords, as well as any technical and administrative information necessary for effective data governance, access, and interpretation.
2.23	Personally Identifiable Information (PII)	Information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.
2.24	Protected Health Information (PHI)	Protected health information (PHI), also referred to as personal health information, is the demographic information, medical histories, test and laboratory results, mental health conditions, insurance information and other data that a healthcare professional collects to identify an individual and determine appropriate care.
2.25	Service Level Agreements (SLA)	A formal document that outlines the expectations between a service provider and the beneficiary.

3.Standard Content

1. Guiding Principles

The following guiding principles form the foundation of the Data Sharing, Integration and Interoperability Standard for the Abu Dhabi Healthcare Ecosystem. These principles are designed to ensure that all data sharing practices within the Abu Dhabi Healthcare Ecosystem are aligned with the overarching goals of improving healthcare quality, enhancing patient safety, and ensuring regulatory compliance.

Patient-Centered Care: All data sharing and interoperability efforts must prioritize the well-being and safety of patients. The exchange of health information should facilitate improved clinical decision-making, enhance patient outcomes, and raise the overall quality of care delivered across the healthcare system.

Security and Privacy: The confidentiality, integrity, and availability of health information are paramount. All data sharing activities must adhere to stringent security protocols and privacy regulations to protect patient data from unauthorized access, breaches, and misuse. This includes compliance with UAE data protection laws and DoH data privacy and security standards, including Abu Dhabi Health Information and Cyber Security Standard.

Interoperability and Integration: The ability of different systems and platforms to work together seamlessly is a core principle of this data domain. Interoperability ensures that health information can be shared and accessed in a timely and accurate manner, regardless of the technology or vendor involved. This supports the DoH's objective of creating a unified, efficient, and

interconnected healthcare system. Adherence to recognized national and international standards is essential to ensure consistency and compatibility across diverse healthcare systems. By following these standards, the DoH ensures that data can be seamlessly exchanged and understood across all entities within the Abu Dhabi Healthcare Ecosystem.

Data Quality and Integrity: All entities within the healthcare ecosystem must ensure that the data they share meet all the characteristics of high-quality data, including completeness, uniqueness, validity, consistency, accuracy and timeliness. By upholding these data quality dimensions, the DoH and entities ensure that high quality data is being shared to support accurate decision-making and reporting. This emphasizes the importance of maintaining data integrity throughout the entire data lifecycle.

Legal and Ethical Compliance: All data sharing practices must comply with the legal, ethical, and regulatory requirements set forth by the UAE government such as the UAE Personal Data Protection Law and the Abu Dhabi Health Data Law. This includes obtaining appropriate patient consent, respecting patient rights, and adhering to data retention and disposal policies.

Transparency and Accountability: All entities participating in data sharing must act transparently by openly communicating their data sharing practices, the purposes for which the data is used, and the roles and responsibilities of each party. Mechanisms for accountability must be established to ensure that all parties comply with the standard and are held responsible for fulfilling their obligations in the data exchange process.

Continuous Improvement and Innovation: The healthcare landscape is continually evolving, and so must the standards that govern data sharing, integration and interoperability. Ongoing evaluation and enhancement of the standards are necessary to incorporate new technologies and innovations, address emerging challenges such as increasing data volumes, user demands and evolving healthcare needs, and improve the overall effectiveness of health information exchange.

2. Standard Statements

Outlined below are the key Standard statements that guide data sharing and interoperability within the Abu Dhabi Healthcare Ecosystem. These statements ensure the responsible management and protection of healthcare data, aligning with established standards and regulations to facilitate secure and efficient data sharing and interoperability internally, externally and with trusted third parties across the ecosystem.

2.1. Data Sharing Governance Framework

2.1.1. The regulatory authority responsible for establishing guidelines and frameworks, as well as governing and enforcing controls for data sharing and interoperability within the DoH and the Abu Dhabi Healthcare Ecosystem, shall be the DoH Data and Digital Governance Office (DoH DDGO).

2.1.2. Entities shall ensure the adoption and development of the Data Sharing Processes, to standardize and streamline data sharing requests internally, externally and with trusted third parties within the Abu Dhabi Healthcare Ecosystem. These processes ensure that data sharing is transparent, secure, and compliant with the regulatory and operational requirements of the healthcare sector.

2.1.3. Any data sharing, internally, externally or with trusted third parties, should be done in accordance with the right Data Classification levels. For details on what data belongs to which classification levels, please refer to the DoH Data Classification Standard[1].

2.1.4. Approvals shall be based on the classification level of the data to be shared as well as whether it is internal within an entity, external or with trusted third parties.

2.1.4.1. **Open Data:**

2.1.4.1.1 Data classified as Open, can be shared internally (within the entity) with limited restrictions and based on the approval channels for each entity.

2.1.4.1.2 Data classified as Open, can be shared externally (outside the entity) or with trusted third parties, and the Data & Digital Governance Office, or its equivalent, shall be responsible for reviewing and approving the data sharing requests.

2.1.4.2. **Confidential Data**:

2.1.4.2.1 For data classified as Confidential, additional approvals will be required for sharing internally (within the entity) for example from the Information Security Team and Privacy teams based on the confidentiality of the data and the applicable data sharing channels.

2.1.4.2.2 For data classified as Confidential, additional approvals will be required for sharing externally (outside the entity) by the DoH as per the authorized delegation of authority based on the confidentiality of the data as well as the applicable data sharing channels, ensuring compliance with all relevant security, privacy, legal and governance standards.

2.1.4.3. **Sensitive Data:**

2.1.4.3.1 For data classified as Sensitive, additional approvals will be required for sharing internally (within the entity) for example from the Information Security Team, Privacy team and Legal team, based on the sensitivity of the data and the applicable data sharing channels, ensuring compliance with all relevant security, privacy, legal and governance standards.

2.1.4.3.2 For data classified as Sensitive, sharing externally (Outside the entity), with third parties, data processors inclusive of counterparts and partners, is not allowed unless authorized by the DoH, as per the DoH governance and security Standards and Policies, and by following the appropriate internal approval channels.

2.1.4.4. **Secret Data:**

2.1.4.4.1 Data classified as Secret must be handled in strict accordance with the DoH security policies and standards. Sharing or exchanging this data, whether physically or digitally is prohibited unless exempted by the DoH delegation of authority and by following established security protocols to ensure confidentiality and compliance.

2.1.5. The DoH shall review and approve specific cases of data sharing requests and address any compliance or ethical issues related to the sharing of sensitive health information, cross-border health data transfers, or data intended for commercial or research purposes.

2.1.6. Entities shall ensure that data labelled with reference to the data classification standard is not transferred, stored, shared, processed or disseminated outside of the UAE, except in cases where a valid and specific exemption is issued by the DoH.

2.1.7. In cases where confidential, sensitive or large volumes of data will be shared outside the entity or with trusted third parties, exemption need to be granted as per DoH authorized delegation of authority and ensuring Data Sharing Agreements (DSAs) are in place, ensuring that these DSAs adhere to all relevant data and information security laws and regulations.

2.1.8. All data sharing must adhere to the DoH's Data Privacy and Protection Standard and Data

Classification Standard, ensuring secure and protected data transfer mechanisms to prevent unauthorized access, breaches, or misuse.

2.1.9. Data shared or exchanged must comply with federal, local and international standards for data interoperability, including healthcare-specific standards where applicable, to ensure compatibility across healthcare systems.

2.1.10. The DoH's DDGO shall conduct periodic reviews of data classifications, in collaboration with the Information and Cybersecurity Team, to ensure alignment with data protection, data security policies, and risk management requirements.

2.1.11. Personal data must be anonymized by default, except when its use in an identifiable form is essential for the specific purpose of data sharing. In cases where identifiable personal data must be shared, appropriate controls and safeguards, such as encryption, access restrictions and defined retention policies, must be implemented to protect the privacy of individuals in accordance with DoH's Data Privacy and Protection Standard.
Personally identifiable information (PII) can only be shared in the following circumstances:

- The data subject has provided explicit consent, as per the DoH's Data Privacy and Protection Standard.
- Data sharing is necessary to fulfill a contractual obligation with the requesting entity, while ensuring compliance with data classification standard.
- Data sharing is required for compliance with a law enforcement investigations or legal obligation to which the entity is subject.
- Data sharing is necessary to protect the vital interests of the data requester or other individuals.
- For any request to share PII that is not explicitly covered by the legal frameworks mentioned above, DoH approval must be obtained through the appropriate data sharing channels based on the classification level of the data, and in compliance with data privacy standards.

2.1.12. If the data is not owned by the entity, the owner of the data must provide written approval granting consent for data sharing. This ensures that data is shared only with proper authorization from its rightful owner.

2.1.13. Entities involved in data sharing are responsible for protecting the data and ensuring that data is strictly used for the defined purposes outlined in the DSA or consent. Data must not be repurposed or misused beyond the agreed terms, ensuring compliance with relevant regulations and standards.

2.2. Data Sharing Request (DSR) Management

2.2.1. The DDGO, or its equivalent, shall establish a Data Sharing Channel to facilitate and manage the submission of data sharing requests within the entity.

2.2.2. The data sharing request template must be defined, developed, and maintained by the DDGO, or its equivalent, to streamline and formalize all data sharing activities.

2.2.3. The data sharing request shall clearly state the following:

- Purpose of Data Sharing: A detailed explanation of the reason for requesting data, specifying for example whether it's for research, healthcare improvement, public health surveillance, or operational needs. It should also specify if the data is for internal use within the entity, or if it will be shared with any external parties.
- Scope of Data Requested: A clear definition of the types and volume of health data being requested.
- Frequency of Data Sharing: Specific intervals or frequency of data exchanges, such as a

one-time exchange, daily, weekly, monthly, annually, or on an ad-hoc basis.
- Duration of Data Use: The defined period during which the data will be needed or utilized.
- Data Format: The preferred format in which the data should be provided.
- Requestor Details: Identification of the organization/department/team and responsible individual submitting the data request.

2.2.4. Comprehensive Data Sharing Controls and standards shall be developed in coordination with the applicable authoritative teams (such as Information Security, Privacy, Legal, etc.). These controls include security protocols, approval workflows, access control, data minimization, anonymization, and audit trails to ensure that all data sharing activities adhere to regulatory and organizational requirements.

2.2.5. Entities must ensure that the requester will adhere to the agreed-upon terms and conditions for data handling within the organization.

2.2.6. The DDGO, or its equivalent, shall ensure that for all applicable DSRs (as specified above in section 2.1) a formal, approved DSA is in place and appropriate approval channels were followed. This process ensures that the terms of use, responsibilities, and restrictions are clearly specified, and that all parties involved fully understand and comply with the agreed-upon conditions for data sharing and handling.

2.2.7. DSA templates must be drafted and reviewed by the Legal Office, or its equivalent, as it is a legally binding document. If the requestor is a trusted third party with an existing DSA, the agreement can be amended to accommodate the new DSR.

2.2.8. All DSAs within the Abu Dhabi Healthcare Ecosystem must clearly outline the terms, conditions, and responsibilities of all parties involved, ensuring compliance with applicable laws and safeguarding the confidentiality, integrity, and security of the shared data. The chosen form of agreement should be appropriate to the nature and sensitivity of the data being shared.

2.2.9. The DDGO, or its equivalent, shall ensure that Data Owners oversee and manage all data sharing requests within their respective data domains.

2.2.10. The Legal Office, or its equivalent, shall handle disputes that arise from the provision of services under the agreement.

2.3. Data Interoperability Framework & Standards

2.3.1. The DoH's DDGO, together with industry representation groups, shall define the Abu Dhabi Healthcare Interoperability Framework, encourage the Abu Dhabi Healthcare Ecosystem to adopt it, and ensure its successful implementation. This framework shall include clear definitions, principles, and goals, establish governance and oversight mechanisms, outline a standardization roadmap, provide technical guidance and support, and incorporate processes for monitoring and evaluation.

2.3.2. The DoH shall establish and maintain processes for the selection, evaluation, and implementation of relevant healthcare data interoperability standards and specifications, and other health data standards.

2.3.3. Entities in the Abu Dhabi Healthcare Ecosystem shall adopt and comply with the DoH data interoperability standards to facilitate efficient and secure health data discovery and exchange among healthcare systems, improving patient safety and advancing public health initiatives.

2.3.4. Entities shall conduct training and capacity building programs for all relevant stakeholders to effectively implement and adhere to the interoperability standards.

2.3.5. DoH DDGO shall ensure regular stakeholder engagement to gather feedback and improve the interoperability framework.
2.3.6. DoH DDGO shall continuously update the interoperability framework and standard to incorporate new technologies and innovations in digital health.

2.4. Data Formats and Structure

2.4.1. Data formats should adhere to interoperability standards where applicable, ensuring that data can be integrated into other systems seamlessly.
2.4.2. All data must be validated and undergo quality checks to ensure accuracy, completeness, consistency, uniqueness, timeliness and validity[2] before sharing or exchanging. This also includes metadata validation to verify the data's integrity. Data must be shared in a format that ensures compatibility and standardization across systems, facilitating efficient and secure data exchange.
2.4.3. Metadata for shared or exchanged data must include, at a minimum: title, description, subject, format, size, publisher, custodian, classification, access permissions, version history, and last updated timestamp. All metadata and associated data in the dataset must be kept up to date to ensure data integrity.
Metadata for shared data can be stored in various ways, including (non-exhaustive):
- Embedded within the data file itself
- In separate metadata files accompanying the data
- In centralized metadata repositories or databases
- Within data sharing platforms

The best approach depends on factors like the type of data, sharing mechanism, and organizational needs. Key considerations include ease of access, security, and maintainability.
2.4.4. For APIs facilitating real-time data exchange, security protocols must be enforced to safeguard data during transmission. Regular monitoring of APIs is required to detect and address potential security breaches or unauthorized access attempts.
2.4.5. The dataset and its metadata should include clear documentation and version control to ensure users are aware of updates or changes.

2.5. Data Integration

2.5.1. The DoH shall establish specific guidelines to govern technical aspects of data integration across the Abu Dhabi Healthcare Ecosystem. This includes integration between DoH and other government entities, integration between healthcare entities, integration by entities to the Health Information Exchange Platform (Malaffi).
2.5.2. These guidelines will focus on ensuring data quality, security, and compatibility with various platforms, supporting seamless data sharing.
2.5.3. A standardized data integration framework shall be defined by the DoH, outlining technical protocols, processes, and best practices for integrating data from multiple sources securely. This framework shall ensure that all data exchanges are compliant with established interoperability standards.
2.5.4. Regular audits of data pipelines, system interfaces, and integration points should be conducted in collaboration with the relevant teams to ensure ongoing compliance with governance and security standards.
2.5.5. API governance protocols should be established, ensuring that all APIs used for data

integration are secure, well-documented, and maintained to facilitate efficient and secure data exchange across systems.

2.5.6. The DDGO, or its equivalent, shall implement data validation and quality assurance mechanisms during integration processes. Real-time error detection mechanisms shall be employed to maintain data integrity.

2.5.7. The DDGO, or its equivalent, shall facilitate collaboration between all relevant teams, including but not limited to Information Security, Data Engineering, Data Stewards, Data Owners and other stakeholders to ensure alignment of data integration efforts with governance standards, security controls, and regulatory requirements.

2.6. Issue and Risk Management

2.6.1. Entities shall establish an issue management framework and a tiered issue classification system to prioritize data sharing and interoperability issues based on severity. Issues shall be designated as high, medium, or low priority, with corresponding response protocols to ensure that resources are efficiently and effectively allocated.

2.6.2. In the event of a high-priority issue related to data sharing or interoperability (e.g., data breach, critical system failure), the Entity shall initiate immediate and decisive action to mitigate risks. The resolution process for high-priority issues shall be expedited to prevent significant impact on healthcare services.

2.6.3. For medium-priority issues related to data sharing or interoperability (e.g., data inconsistencies, integration challenges), the DDGO, or its equivalent, shall engage in a systematic and timely resolution process, ensuring that these concerns are addressed promptly while managing the effective distribution of attention and resources.

2.6.4. Low-priority issues related to data sharing or interoperability shall be managed in a way that ensures they are addressed within a reasonable timeframe, without diverting critical resources from higher-priority concerns, but with sufficient attention to prevent escalation.

2.6.5. The DoH's DDGO shall design an escalation hierarchy for raising data-related risks and issues associated with data sharing and interoperability through a centralized mechanism, ensuring effective management and resolution of such concerns.

2.6.6. The DDGO, or its equivalent, shall document and track all data-related issues and resolutions in a governance register to ensure transparency and accountability. The register's format and accessibility shall be defined to facilitate efficient data management and oversight.

3. Change Management

3.1.1. Healthcare ecosystem entities shall implement a change management plan to support the adoption of data and digital standards. This plan shall cover at minimum, but not limited to:

- Communication: clear strategy to inform stakeholders of goals and updates of the plan
- Training: interactive sessions on standards, protocols, and tools for all users
- Awareness: ongoing campaigns to reinforce the value of data & digital standards
- Monitoring: regular evaluation of the plan's effectiveness and adjustments as needed

3.1.2. The DDGO, or its equivalent, shall enforce standards for compliance monitoring to support reliable data for decision-making and digital transformation.

4.Key stakeholder Roles and Responsibilities

Stakeholder Name	Stakeholder Key Role
DoH's Data and Digital Governance Office (DoH's DDGO)	-Define and enforce data sharing, integration, and interoperability standards across the Abu Dhabi Healthcare Ecosystem. -Ensure compliance with DSAs and relevant data laws in collaboration with the Information Security and Legal team. -Oversee internal and external data sharing requests and ensure correct approval channels are followed based on Data Classification Levels and security standards. -Define data integration standards. -Manage the Abu Dhabi Healthcare Interoperability Framework to promote seamless data sharing. -Develop and implement training programs to promote adoption of data sharing and interoperability standards. -Regularly review adherence to governance standards and audit data sharing processes. -Establish a framework for managing and resolving data sharing and interoperability issues.
Entity Data and Digital Governance Office (DDGO)	-Implement data governance standards and frameworks set by DoH's DDGO. -Manage internal and external data sharing requests, ensuring compliance with DSAs and security policies. -Collaborate with Information Security, Legal, and committees for proper data handling and integration. -Establish and maintain data sharing channels for efficient request management. - Ensure the correct approval channels are followed based on the classification of data to be shared. -Monitor data integration frameworks to ensure operational data flows.
Information Security Team	-Establish and implement security controls for data sharing, including encryption and access management. -Collaborate with DDGO to review and approve data sharing requests, ensuring security measures based on data classification. -Monitor data sharing to detect and address security breaches or unauthorized access. -Conduct regular security assessments and audits to ensure compliance with protocols. -Ensure compliance with data protection laws for all internal and external data sharing.
Legal Office	-Draft, review, and approve DSA templates for external data sharing, ensuring legal and regulatory compliance. -Address and resolve disputes related to DSAs and agreements. -Ensure all data sharing agreements and practices comply with UAE and Abu Dhabi data laws.
Data Governance Specialist	-Record and track data sharing requests, including DSAs, consents, and amendments, ensuring compliance. -Monitor compliance with SLAs, security standards, and regulations, escalating issues when needed. -Assist in identifying, tracking, and resolving data-related issues, ensuring timely closure.
Data Owner	Ensures data quality and coordinates the communication between stakeholders involved in the data sharing process.
Data Steward	Ensures that the data meets quality standards through data quality checks and communicating the details of the DSR to the Data Custodian for data preparation.
Data Custodian	Manages the secure retrieval, preparation, and transfer of data, ensuring compliance with security and privacy requirements.

5.Monitoring and Evaluation

The entity shall establish a robust monitoring system to track and evaluate compliance with the standard. This includes using reliable metrics and measurements to assess the effectiveness of the implemented controls. The entity will periodically report its compliance status, any deviations, and associated risks to the DoH. Risks related to non-compliance must be recorded and managed appropriately. Regular internal audits and assessments must be conducted to validate and verify compliance with the standard's requirements. Based on the outcomes of these monitoring and evaluation activities, the entity must establish a continuous improvement process to adapt to emerging threats, technological changes, and evolving compliance requirements. Additionally, the DoH will conduct periodic audits and technical assessments of all regulated entities, as relevant and applicable, to ensure compliance with the standard.

6.Enforcement and Sanctions

DoH may impose sanctions in relation to any breach of requirements under the Data Sharing, Integration and Interoperability Standard in accordance with the Disciplinary Regulations of the Abu Dhabi Healthcare Sector governed by the UAE federal laws.

7. Relevant Reference Documents

No.	Reference Date	Reference Name	Relation Explanation / Coding / Publication Links
1.	2025	Data Classification Standard	https://www.doh.gov.ae/en/resources/standards
3.	2025	Data Quality Standard	https://www.doh.gov.ae/en/resources/standards