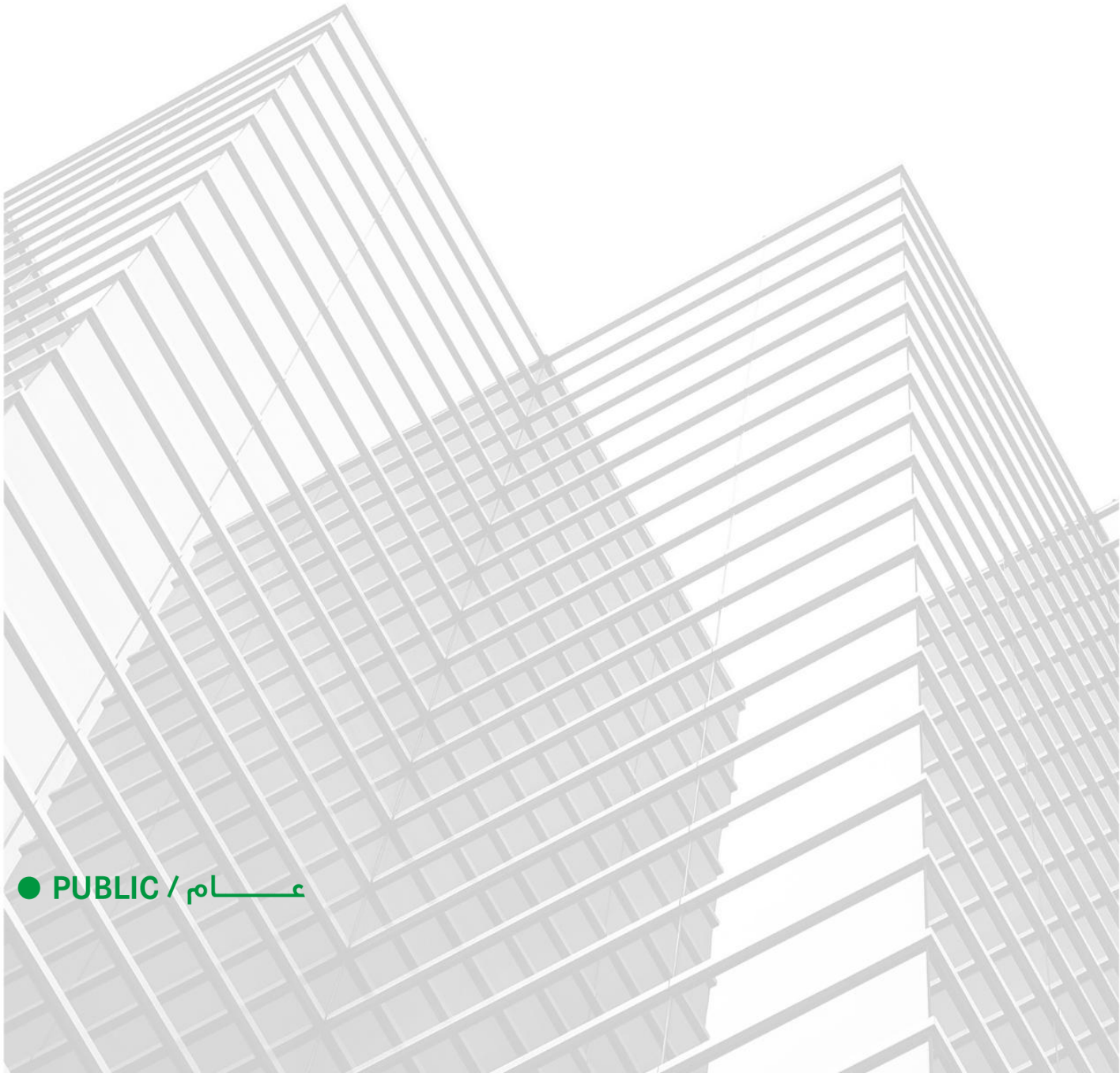
دائـــــرة الـصـــحـــة
DEPARTMENT OF HEALTH

# ANALYTICS & REPORTING STANDARD



● PUBLIC / عـــــــام

| | | | |
|---|---|---|---|
| Document Title: | Analytics & Reporting Standard | | |
| Document Ref. Number: | DoH/ST/DDGO/AR/V1/2026 | Version: | 1 |
| New / Revised: | New | | |
| Publication Date: | April 2026 | | |
| Effective Date: | May, 2026 | | |
| Document Control: | Strategy Sector | | |
| Applies To: | All DoH Offices, Centers, Sectors & Organization Unit, DoH ecosystem | | |
| Owner: | Data & Digital Governance Office | | |
| Revision Date: | Feb 2029 | | |
| Revision Period: | Every three years | | |
| Contact: | DDG@doh.gov.ae | | |

## 1. Standard Purpose and Brief

The purpose of the Analytics and Reporting Standard is to establish a baseline and guidelines for collecting, analyzing, interpreting, and presenting healthcare data within Department of Health (DoH) and all ecosystem entities that are using data for analytics and reporting. By enabling effective use of data and establishing business intelligence (BI) use cases, stakeholders can interpret and compare data accurately, leading to better decision-making and improved healthcare system outcomes.

The Analytics and Reporting Standard also address the secondary use of data, ensuring that any data repurposed beyond its original intent is handled in a manner that complies with privacy regulations, maintains data integrity, and supports research, quality improvement, and policy development initiatives within the healthcare ecosystem.

The DoH and all ecosystem entities rely on analytics and reporting to make informed decisions and improve the healthcare system, hence the need for reliable data and standardized reporting.

This Standard is implemented in conjunction with following Protocols

- Annex A- BI & Analytics Use Case Validation Protocol
- Annex B- BI Ethical Use Risk Mitigation Protocol
- Annex C- Identify and Collect Data for Reporting Protocol

## 2. Definitions and Abbreviations

| No. | Term / Abbreviation | Definition |
|---|---|---|
| 2.1 | Abu Dhabi Healthcare eco-system | Organizations, institutions, and stakeholders involved in delivering, managing, regulating, or supporting healthcare services, regulated by DoH. This includes healthcare providers, hospitals, clinics, research institutions, and any affiliated organizations that contribute to or interact with healthcare data, digital health services, and patient care within Abu Dhabi. These entities are responsible for adhering to the policies, regulations, and standards established by the Department of Health (DoH). |
| 2.2 | Business Intelligence (BI) | Processes, technologies, and strategies to analyze and interpret data, with the goal of gaining actionable insights and making informed decisions. |
| 2.3 | Data and Digital Governance Office (DDGO) | A centralized unit responsible for overseeing the management, security, and ethical use of data and digital assets. The DDGO drives strategies to improve data and digital governance, standardize practices, and align both with the organization's overall data and digital objectives. |
| 2.4 | Department of Health (DoH) | The regulatory authority responsible for overseeing healthcare operations within the Abu Dhabi healthcare ecosystem.<br>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. |

| | | |
|---|---|---|
| **2.5** | Patient | An individual receiving healthcare services, who owns their personal health information and provides consent for its usage as per data governance regulations. |
| **2.6** | Personal Data | Any information that relates to an identifiable individual. This includes data that directly identifies a person, such as their name, identification number, or contact details, as well as information that can indirectly identify a person when combined with other data, such as location data, IP addresses, or specific attributes like age, gender, or health records. |
| **2.7** | 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. |
| **2.8** | Protected Health Information (PHI) | Any information in a healthcare setting that can be used to identify an individual and relates to their medical history, treatment, or payment for healthcare services. |
| **2.9** | Secondary Use of Data | The practice of using data for purposes other than its original intent. Data initially collected for primary purposes, like patient care or clinical trials, is repurposed for additional objectives, such as research, quality improvement, public health response, regulatory documents development, or commercial activities. |

## 3. Standard Purpose and Brief

### 3.1. Guiding Principles

Adhering to the DoH's values of accountability, excellence, integrity and trust, the following guiding principles are established to lead data & digital analytics and reporting activities:

3.1.1. **Confidentiality & Privacy:** Maintain the confidentiality of health information and protect patient privacy from unauthorized access or disclosure through measures such as access controls, encryption, and privacy compliance. Implement strict data de-identification and anonymization techniques in analytics, reporting, and secondary use of data. Limit access to sensitive data to authorized personnel only and ensure compliance with local ADHICS Standard and other applicable UAE federal laws, Abu Dhabi and DoH regulations, and relevant legal frameworks.

3.1.2. **Data Quality:** Ensure the accuracy, completeness, uniqueness, timeliness and reliability of data used in healthcare analytics to support patient safety and care quality. Implement rigorous data validation processes, regular audits, and standardized data entry protocols to maintain high data quality standards.

3.1.3. **Patient consent and autonomy:** Respect patient autonomy by ensuring informed consent for the use of their data in analytics, reporting and secondary use of data. Data usage must align with patient preferences and privacy rights and opt-out options must be clearly communicated and easily accessible.

3.1.4. **Patient-centric:** Ensure that analytics and reporting efforts are focused on improving patient outcomes, safety, and care quality. Prioritize data projects that provide actionable insights for patient care, reduce errors, and enhance clinical decision-making.

3.1.5. **Data-driven decision-making:** Utilize data analysis and interpretation to generate actionable insights and recommendations, ensuring objectivity and accuracy. Adopt a cycle of continuous learning and improvement by collecting data, analyzing outcomes, and adjusting strategies based on the insights gained from data-driven analysis.

3.1.6. **Ethical Use of Data:** Avoid using data in ways that could lead to discriminatory practices or negatively impact patient trust. Ensure data usage aligns with the core values of patient care and safety.

### 3.2. Standard Statements

Outlined below are the fundamental statements governing the analytics and reporting of data.

#### 3.2.1. Strategy & Plan

The DoH and Healthcare ecosystem entities that have established an analytics function shall:

3.2.1.1. Design Analytics and Reporting Strategy which align with overall strategic goals and priorities supporting patient outcomes, public health interventions and initiatives, enhancing operational efficiency and ensuring regulatory compliance.

3.2.1.2. Ensure that an Analytics and Reporting roadmap is developed in alignment with data and digital governance standards and protocols and shall have oversight on the prioritization of analytics use ensuring consistency with overall data and digital strategy of the organization.

3.2.1.3. Identify and prioritize a list of analytics use cases based on their potential to drive improvements in patient care, operational efficiency, and organizational performance.

3.2.1.4. Align use cases for analytics and reporting with the strategic goals and priorities of the entity supporting initiatives such as population health management, value-based care, and quality improvement.

3.2.1.5. Regularly review and update the use case portfolio. This ensures that the portfolio remains current and aligned with evolving organizational needs. The review shall include

the following activities, among others:

3.2.1.5.1. Reviewing and adjusting the status of use cases within the portfolio.

3.2.1.5.2. Evaluating the planned use cases in the portfolio to assess their relevance.

3.2.1.5.3. Identifying new use cases through ideation workshops.

3.2.1.5.4. Reassessing the prioritization of existing use cases and prioritizing new ones.

3.2.1.6. Ensure that all analytics use cases are accurately recorded in the entity's repository and adhere to a uniform documentation. Ethical considerations and governance shall be integrated into the review and approval process for analytics use cases, ensuring compliance with relevant standards and regulations.

3.2.1.7. Ensure that Business Intelligence, Data Science and AI team embeds ethical data use and system development at every stage of AI System Lifecycle.

### 3.2.2. Analytics Tools and Platform

The DoH and Healthcare ecosystem entities that have established an Analytics function shall:

3.2.2.1. Prioritize the use of approved and recommended analytics tools which are compatible with the existing data infrastructure to facilitate seamless integration and data exchange.

3.2.2.2. Establish criteria for selecting analytics tools and platforms based on factors such as functionality, scalability, interoperability, security, and compliance with regulatory requirements.

3.2.2.3. Ensure that analytics tools and platforms adhere to strict data security standards and protocols to protect healthcare information from unauthorized access, breaches, or misuse.

3.2.2.4. Ensure that adequate training and support services are provided to users of analytics tools and platforms to ensure that they are proficient in using the tools effectively and maximizing their capabilities for data analysis and reporting.

3.2.2.5. Ensure that analytics tools and platforms support data visualization capabilities, including interactive dashboards, charts, graphs, and reports, to enable users to explore and communicate insights effectively.

3.2.2.6. Use uniform data analysis tools and methodologies to ensure consistent and reliable reporting.

### 3.2.3. Data Collection and Curation

The DoH and Healthcare ecosystem entities that have established an Analytics function shall:

3.2.3.1. Ensure that Data Governance specialist or equivalent establishes and enforces data quality rules and conducts regular quality audits

3.2.3.2. Identify and document all data sources used for analytics and reporting, including internal systems, external databases, third-party sources, and IoT (Internet of Things) devices. Controls must be set to ensure that data at source is not manipulated.

3.2.3.3. Develop a data sourcing plan defining clear objectives and milestones to guide the implementation of use cases initiatives.

3.2.3.4. Define clear data requirements for each use case, specifying the types of data needed, data sources, data quality standards, and data governance considerations to ensure that the necessary data is available and accessible for analysis.

3.2.3.5. Ensure the quality of data before it is used for analytics or reporting purposes.

3.2.3.6. Comply with applicable laws, regulations, and industry standards, including but not limited to privacy laws and data security requirements.

3.2.3.7. Ensure that standardized procedures and protocols are followed for data collection cleaning, preprocessing, transformation, and normalization to prepare data for analysis and reporting.

### 3.2.4. Data Reporting

DoH and Healthcare ecosystem entities that have established an Analytics function shall:

3.2.4.1. Ensure that healthcare data reports are accurate, reliable, and timely, reflecting the most current information available and meeting designated deadlines for reporting.

3.2.4.2. Adhere to relevant healthcare regulations, privacy, and security laws, ensuring the protection of patient confidentiality and data privacy.

3.2.4.3. Ensure that reports are tailored to the specific needs of stakeholders, presented in a clear, standardized and actionable format, and visualized effectively for better comprehension.

3.2.4.4. Ensure transparency, accountability, and traceability throughout the data reporting processes, including methodologies and outcomes.

3.2.4.5. Ensure that all aspects of data analysis and interpretation processes, including assumptions, methodologies, limitations, and conclusions, are documented effectively to promote transparency, accountability, and reproducibility.

3.2.4.6. Ensure that analytics and reporting activities of internal and external data are protected, follows data access, data sharing and data privacy policies, ensuring confidentiality and data masking where applicable.

### 3.2.5. Data Calculation

3.2.5.1. A standardized calculation method shall be established for calculating and reporting across the organization to enhance user confidence in the entity's reports. This approach will ensure data comparability, facilitate meaningful analysis of trends and performance across the entity's programs and departments, and promote transparency and accountability in corporate, clinical and public health reporting.

3.2.5.2. Documentation shall specify the exact calculation formula, data sources, and any relevant data transformations required.

3.2.5.3. Deviations from the standardized calculation method shall only be permitted under exceptional circumstances and with prior written approval as per a governed delegation of authority within the entity.

3.2.5.4. Any approved deviations shall be clearly documented and reported alongside the reported data.

3.2.5.5. Documentations shall be reviewed and updated periodically, but not less than once a year, to reflect changes in data sources, calculation methods, or reporting requirement.

### 3.2.6. Secondary Use of Data

3.2.6.1. The secondary use of reported data shall be authorized and managed in accordance with the ADHICS, Data Classification Standards, and other DoH regulations. The use of open data for secondary purposes is permitted without restrictions, whereas confidential, sensitive and secret data, including Personally Identifiable Information (PII) and Protected Health Information (PHI), shall require appropriate approvals in line with the Data Classification Standard.

#### 3.2.6.2. Permitted Use

3.2.6.2.1. All patient data used for secondary purposes must be anonymized or de-identified to protect patient privacy and confidentiality, unless explicitly permitted by the patient or required by law.

3.2.6.2.2. Secondary use of patient data shall be permitted for research and educational purposes, such as case studies, simulations, or training healthcare professionals, if patient identities are protected.

3.2.6.2.3. Secondary use of patient data shall be permitted for public health purposes, such as tracking disease outbreaks, evaluating healthcare interventions, or conducting preventive and curative procedures related to public health or patient health and safety, if patient identities are protected.

3.2.6.2.4. Secondary use of health data, genetic information, or any personal data with the purpose of denying or limiting access to insurance coverage, employment opportunities, financial services, housing, education, or other essential services and benefits, shall be prohibited.

3.2.6.2.5. Secondary use of PII data for commercial gain shall be prohibited without explicit consent from the data subjects.

3.2.6.2.6. Attempting to re-identify individuals from anonymized or de-identified data sets shall be prohibited, as it breaches privacy and ethical standards.

3.2.6.2.7. The secondary use of patient data shall be permitted without patient consent if requested by a competent judicial authority.

**3.2.6.3. Security and Privacy**

3.2.6.3.1. DoH and all healthcare ecosystem entities shall implement robust security measures, including encryption, access controls, and regular audits, to protect patient data used for secondary purposes against unauthorized access, breaches, and misuse.

3.2.6.3.2. The minimum necessary amount of data required to achieve the specific secondary purpose shall be accessed or used, ensuring that excess data exposure is avoided.

3.2.6.3.3. Healthcare ecosystem entities must obtain explicit informed consent from patients before using their data for secondary purposes. Patients must be informed about the specific secondary use, the potential risks, benefits, and the option to opt-out without any impact on their care.

3.2.6.3.4. Patients have the right to withdraw their consent for the secondary use of their data at any time, and such requests shall be honored promptly without any impact on the quality of care provided.

**3.2.6.4. Data Sharing**

3.2.6.4.1. Any sharing of patient data with third parties for secondary use shall be governed by a formal data sharing agreement that specifies the data to be shared, the purpose of use, security measures, and accountability for data protection and compliance.

3.2.6.4.2. Sharing data with third parties who do not comply with data protection regulations or who use the data for unauthorized purposes shall be prohibited.

**3.2.6.5. Retention**

3.2.6.5.1. Data used for secondary purposes shall be retained only for as long as necessary to fulfill the stated purpose. Once the purpose is achieved, data shall be securely disposed of or returned to its original format if re-identification is required for primary use.

**3.2.6.6. Ethics**

The DoH and Healthcare ecosystem entities that have established an Analytics function shall:

3.2.6.6.1. Ensure that data is used equitably, without perpetuating or reinforcing biases, discrimination, or disparities in healthcare services. Special consideration must be given to vulnerable populations to avoid unintentional negative impacts.

3.2.6.6.2. Maintain full transparency regarding the legal and ethical requirements related to secondary use of data, ensuring that stakeholders, including patients and external partners, are informed of how their data is being used, the purpose of use, the potential risks, and expected benefits.

3.2.6.6.3. Be held accountable for the ethical use and protection of data in secondary use cases. Data misuse, improper handling, or any violations of established standards shall be subject to strict legal sanction.

3.2.6.6.4. Implement bias detection and mitigation techniques to ensure that outcomes are fair, impartial, and beneficial to all groups.

3.2.6.6.5. Establish mechanism for publicly disclosing the secondary use of data in major projects or research initiatives, providing stakeholders with information on how data is used to drive public health improvements, system optimization, and service delivery advancements.

3.2.6.6.6. Designate responsible parties, such as analytics use case owners, who will be accountable for the appropriate and ethical handling of data in secondary use cases. These roles ensure that all ethical, regulatory, and operational standards are upheld throughout the data lifecycle.

3.2.6.6.7. Implement risk management frameworks to evaluate the potential ethical risks associated with the secondary use of data. This includes assessing how data use may impact patient privacy, public trust, and societal equity, and implementing mitigations as necessary.

### 3.2.7. Issue and Risk Management

The DoH and Healthcare ecosystem entities that have established an Analytics function shall:

3.2.7.1. Identify and manage risks related to the privacy of patient information, certain disease data, financial data among others, the risks including unauthorized access, disclosure, or misuse of sensitive healthcare data during analytics, and reporting processes.

3.2.7.2. Identify and manage risks related to data security, including vulnerabilities in systems, networks, and applications used for analytics and reporting, as well as potential threats such as cyberattacks, malware, and insider threats.

3.2.7.3. Establish incident response plans and contingency measures to address potential risk incidents, including data breaches, security breaches, compliance violations, and other adverse events, with procedures for reporting, investigation, and remediation.

3.2.7.4. Oversee anonymization and de-identification techniques, ensure data minimization (only use the necessary data), and regularly audit data practices to detect any potential breaches of privacy.

3.2.7.5. Implement clear and transparent consent processes that inform individuals about potential secondary uses of their data. Dynamic consent models that allow individuals to update their preferences over time shall be utilized.

3.2.7.6. Ensure that Data quality checks and validation processes are implemented and adhered to by relevant departments before data is used for secondary purposes.

## 3.3. Change Management

The DoH and Healthcare ecosystem entities that have established an Analytics function shall:

3.3.1 Implement a change management plan to support the adoption of data and digital standards. This plan shall be addressed at minimum, but not limited to:

3.3.1.1 **Communication**: clear strategy to inform stakeholders of goals and updates of the plan.

3.3.1.2 **Training**: interactive sessions on standards, protocols, and tools for all users.

3.3.1.3 **Awareness**: ongoing campaigns to reinforce the value of data & digital standards.

3.3.1.4 **Monitoring**: regular evaluation of the plan's effectiveness and adjustments as needed.

3.3.2 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 |
|---|---|
| Business Intelligence Team | Design integrated platforms tailored to organizational needs. |
| | Use approved analytics tools aligned with existing infrastructure. |
| | Provide tools for data visualization (dashboards, reports). |
| | Oversee lifecycle and performance of BI use cases. |
| | Establish standardized calculation and reporting methods in collaboration with business owners. |
| | Manage a repository of the calculation and reporting methods. |
| | Establish methodologies and models for BI data analysis. |
| Data Sciences & AI Team | Oversee AI use cases throughout their lifecycle. |
| | Review and reprioritize use cases semi-annually. |
| | Use predictive models to optimize patient care and operations. |
| | Ensure interdisciplinary collaboration and ethical data use. |
| | Establish methodologies and models for AI data analysis. |
| DoH's Data and Digital Governance Office (DoH's DDGO) | Align analytics initiatives with DoH objectives. |
| | Oversee data governance and ensure ecosystem compliance. |
| | Develop training programs for ecosystem entities. |
| | Optimize analytics tools and processes. |
| Data and Digital Governance Office (DDGO) | Develop strategies and ensure data consistency and governance. |
| | Ensure regulatory and ethical compliance in data use. |
| | Lead awareness initiatives and implement change processes. |
| | Oversee KPIs, track performance, and ensure corrective actions. |
| Data Governance Specialist | Establish and enforce data quality rules for analytics and reporting. |
| | Conduct regular audits to ensure adherence to data governance standards. |
| | Review and approve the ethicality of data use cases before development. |
| | Assist in managing data lifecycle, ensuring compliance with governance policies. |
| | Provide guidance and training on data governance practices. |
| Information & Cybersecurity Team | Enforce data security protocols and protect against breaches. |
| | Implement incident response and risk mitigation strategies. |
| | Ensure data anonymization and secure secondary use. |
| | Audit and monitor data access and security compliance. |
| Analytics Use Case Owner | Oversee execution, monitoring, and performance. |
| | Establish and track key performance metrics. |
| | Validate data accuracy and compliance. |
| | Identify and mitigate risks in data privacy and security. |

## 5. Monitoring and Evaluation

5.1 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

6.1 DoH may impose sanctions in relation to any breach of requirements under the Data Storage & Retention 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 | 11/2025 | Data Access Standards | https://www.doh.gov.ae/en/resources/standards |
| 2 | 11/2025 | Data Classification Standard | https://www.doh.gov.ae/en/resources/standards |
| 3 | 11/2025 | Data Sharing and Interoperability Standard | https://www.doh.gov.ae/en/resources/standards |
| 4 | 11/2025 | Ecosystem Data Governance Standard | https://www.doh.gov.ae/en/resources/standards |
| 5 | 11/2025 | Identify & Collect Data for Reporting Protocol | https://www.doh.gov.ae/en/resources/standards |
| 6 | 11/2025 | Business Intelligence and Analytics Use Case Validation Protocol | https://www.doh.gov.ae/en/resources/standards |
| 7 | 11/2025 | BI Ethical Use Risk Mitigation Protocol | https://www.doh.gov.ae/en/resources/standards |
| 8 | 06/2024 | ADHICS V2 | https://www.doh.gov.ae/en/resources/standards |