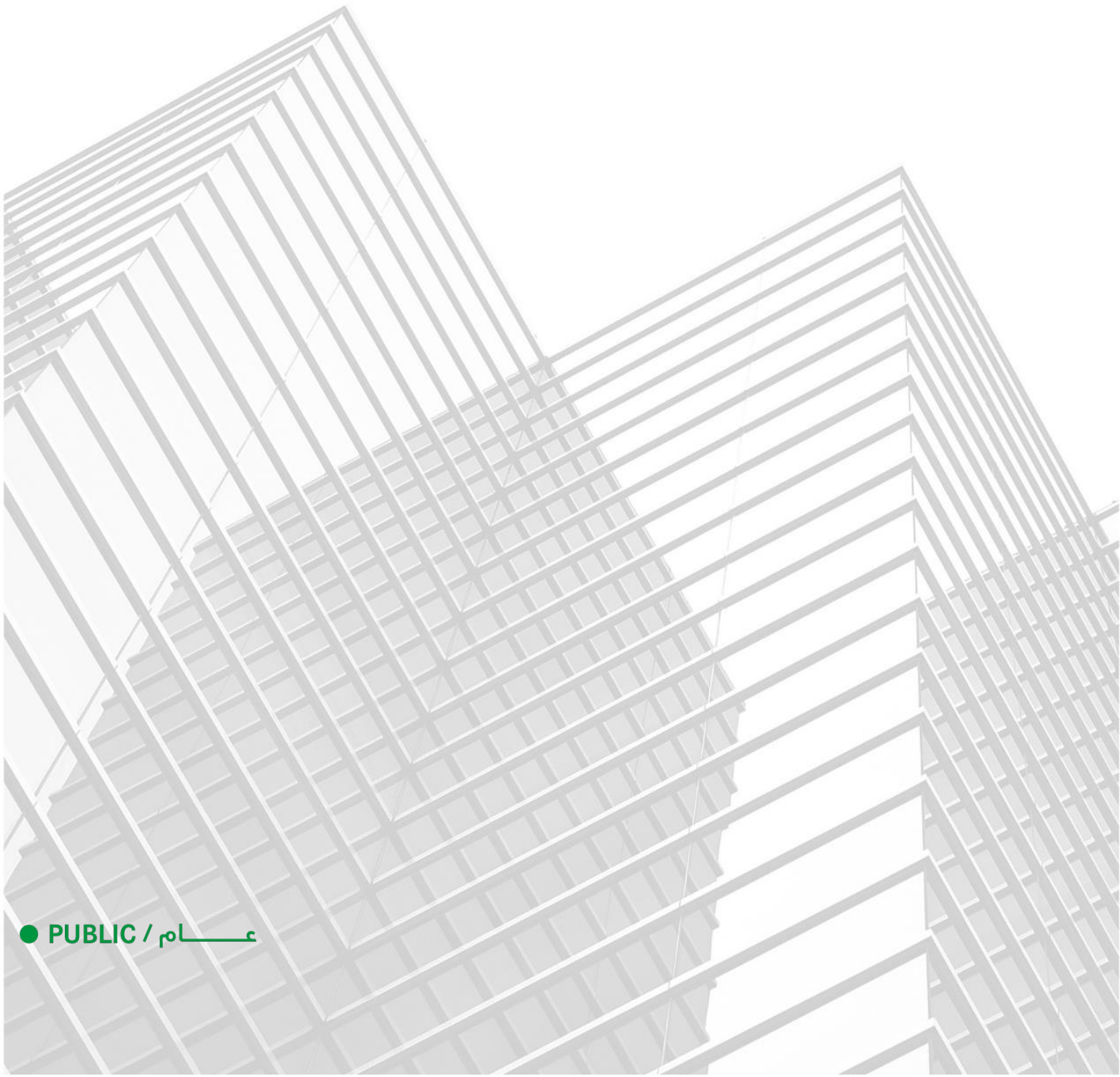
دائـــــرة الـصـــحـــة
DEPARTMENT OF HEALTH

# RESPONSIBLE ARTIFICIAL INTELLIGENCE (AI) STANDARD



● PUBLIC / عـــــــام

| | | | |
|---|---|---|---|
| Document Title: | Responsible Artificial Intelligence (AI) Standard | | |
| Document Ref. Number: | DoH/ST/DDGO/RAI/V1/2025 | Version: | V1 |
| New / Revised: | New | | |
| Publication Date: | Oct 2025 | | |
| Effective Date: | Oct 2025 | | |
| Document Control: | Strategic Affairs Sector | | |
| Applies To: | All DoH Offices, Centers, Sectors & Organization Units, Abu Dhabi Healthcare ecosystem | | |
| Owner: | Data and Digital Governance Office | | |
| Revision Date: | Oct 2026 | | |
| Revision Period: | One year | | |
| Contact: | DDG@doh.gov.ae | | |

## 1. Standard Scope

1.1. In alignment with the guiding principles and strategic pillars articulated in the DoH AI Policy, the following standard represents the minimum requirements to operationalizing responsible AI across healthcare eco-system in Abu Dhabi. These statements serve to translate policy ideals into actionable directives, ensuring that AI technologies are not only technically robust but also socially responsible and continuously evaluated for well-being and safety of patients and the community.

1.2. The standard applies to the DoH and all licensed healthcare entities within the Emirate of Abu Dhabi that are engaged in the development, procurement, or deployment of artificial intelligence (AI) systems. It pertains to AI-enabled tools, devices, datasets, agents, platforms employed for clinical, financial, administrative and other related functions. It applies to AI systems developed internally, sourced from third-party vendors, or created through research collaborations, covering the entire lifecycle from inception and deployment to decommissioning.

1.3. The Standard is divided into 4 sections

1.3.1. Core Foundations for all AI systems

1.3.2. Data Management for AI

1.3.3. AI Risk Management

1.3.4. AI Literacy

1.4. A comprehensive detailing of the Risk management process is outlined in the Responsible AI-Risk Management Protocol.

## 2. Definitions and Abbreviations

| No. | Term / Abbreviation | Definition |
|---|---|---|
| **2.1** | Abu Dhabi Healthcare Ecosystem | 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** | Artificial Intelligence (AI) | The simulation of human intelligence in machines designed to perform tasks that typically require human cognitive functions, such as learning, reasoning, problem-solving, understanding natural language, and adapting to new inputs. AI systems use algorithms and data to make decisions, recognize patterns, and improve performance over time. |

| | | |
|---|---|---|
| **2.3** | AI Systems | Systems, solutions, models, tools, and data (including training, validation, and testing data) that are designed, developed, collected, acquired, re-purposed, or otherwise procured in order to be used in connection with AI for internal use, direct patient care, healthcare research and development, and any other purpose. |
| **2.4** | Data Users | Individuals or organizations that utilize a dataset during any stage of the lifecycle of an AI health technology. |
| **2.5** | DoH's Data and Digital Governance Office (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. |
| **2.6** | Department of Health (DoH) | The regulative body of the Healthcare Sector in the Emirate of Abu Dhabi, Established based on law No. (10) of 2018 |
| **2.7** | Legal Affairs Sector | A sector within DoH responsible for handling legal matters, ensuring compliance with applicable laws, regulations, and agreements. |
| **2.8** | Responsible AI | The practice of designing, developing, and deploying AI systems in a manner that is ethical, transparent, accountable, and respects human rights and values. It aims to ensure that AI benefits society while minimizing potential harm and risks. |
| **2.9** | Privacy by Design | An approach where privacy is integrated into the design and architecture of systems from the outset, ensuring that personal data protection is a fundamental part of system development. |
| **2.10** | Residual Risk | The remaining level of risk after mitigation actions have been applied to reduce the potential impact or likelihood of a risk occurring. |
| **2.11** | Risk Assessment | The systematic process of identifying, analyzing, and evaluating risks to determine their potential impact and likelihood, often used for decision-making on risk mitigation. |
| **2.12** | Risk Mitigation | Actions or strategies implemented to reduce or eliminate the likelihood or impact of identified risks to acceptable levels. |
| **2.13** | Risk Register | A documented log of identified risks, including their severity, likelihood, mitigation measures, and monitoring status, used to track and manage risks throughout a project or system lifecycle. |

## 3. Standard Requirements and Specifications

### 3.1 Core Foundations

3.1.1 **Human Centered Design:** AI systems shall be designed and deployed to complement human capabilities by enhancing decision-making, creativity, and judgment. AI systems must preserve and support the essential human qualities of empathy and care, ensuring that technology augments rather than replaces the human element.

3.1.1.1 Empathy and Care

3.1.1.1.1 AI systems must be co-designed with meaningful participation from clinicians, patients, and technologists to ensure relevance and usability.

3.1.1.1.2 AI must account for personal factors, moving beyond one-size-fits-all algorithms toward tailored interventions and equitable outcomes.

3.1.1.1.3 AI systems must seamlessly integrate into existing medical workflows to ensure clinical efficiency is not hindered or disrupted.

3.1.1.2 Human Oversight and Escalation

3.1.1.2.1 AI systems shall incorporate human-in-the-loop or human-on-the-loop mechanisms to ensure appropriate oversight and intervention where necessary.

3.1.1.2.2 AI systems must always function under human oversight. Clear escalation protocols shall be established within AI systems, outlining specific actions and decision points based on varying risk levels to involve human oversight effectively.

3.1.2 **Safety and Integrity:** AI systems must be resilient to errors, malfunctions, and inconsistencies that could impact patient care or compromise clinical outcomes. AI systems must operate under effective human oversight, uphold the highest standards of safety, and demonstrate robust performance across their lifecycle.

3.1.2.1 Robustness

3.1.2.1.1 AI models must be designed to operate reliably under variable conditions, including infrastructure failures and adversarial threats

3.1.2.1.2 Systems must include graceful degradation mechanisms and fallback procedures to ensure continuity of care in the event of partial failure.

3.1.2.1.3 Safety testing and failure mode analyses must be done before deployment and monitored continuously for anomalies.

3.1.2.1.4 Post deployment systems must be monitored continuously for performance degradation, anomalies, and unintended consequences, with automated alerts and manual review triggers.

3.1.2.2 Continuous Feedback and Improvement

3.1.2.2.1 AI systems must incorporate feedback mechanisms that enable continuous performance monitoring, error detection, and iterative improvement.

3.1.2.2.2 Feedback loops shall include both automated and human-in-the-loop processes to capture system outputs, user interactions, and real-world outcomes for model refinement and risk mitigation.

3.1.3 **Accuracy and Reliability:** AI models must be rigorously validated against established performance benchmarks to ensure they meet required standards. Models should be continuously monitored to maintain accuracy and detect any deviations over time.

3.1.3.1 Performance Assessment

3.1.3.1.1 AI models shall undergo rigorous validation against established performance benchmarks before deployment to ensure compliance with relevant standards and reliability criteria.

3.1.3.1.2 Validation processes must include comprehensive testing across diverse datasets and contexts to confirm accuracy, safety, and efficacy.

3.1.3.1.3 Post-deployment, AI models shall be continuously monitored using automated systems and periodic assessments to identify and address any performance deviations or anomalies.

3.1.3.1.4 Any significant decline in model performance or unexpected behaviors must trigger review and corrective action in accordance with organizational protocols.

3.1.3.1.5 Documentation of validation results and ongoing performance monitoring must be maintained for audit and accountability purposes.

3.1.4 **Data Privacy and Cybersecurity:** Safeguard the confidentiality, integrity, and availability of all AI systems through robust cybersecurity and data privacy practices. AI technologies must be designed, deployed, and maintained in accordance with secure-by-design principles, ensuring protection across every layer of system architecture and aligned with the Information and Cybersecurity requirements defined under prevailing applicable laws and regulations including Abu Dhabi Healthcare Information and Cyber Security (ADHICS) Standard.

3.1.4.1 Security and Privacy Governance

3.1.4.1.1 A formal governance structure must oversee AI security and privacy, including defined roles, policies, risk assessments, and continual improvement mechanisms.

3.1.4.1.2 AI systems must be architected with layered defenses, threat modeling, and secure development lifecycles that address adversarial risks and system vulnerabilities.

3.1.4.2 Access Control

3.1.4.2.1 Role-based access controls, multi-factor authentication, and least-privilege principles must be enforced across all AI components, including data, models, and APIs.

3.1.4.2.2 All access to AI systems—including but not limited to data, models, APIs, and administrative interfaces, must be governed by role-based policies, enforced through multi-factor authentication and regularly reviewed to ensure appropriateness.

3.1.4.2.3 Users and systems must operate under the principle of least privilege, with only the minimal necessary access granted, time-bound privileges monitored, and all activity logged for audit and compliance purposes.

3.1.4.3 Software Code Reviews and Maintenance

3.1.4.3.1 All proprietary and third-party AI software must undergo formal secure code reviews and automated vulnerability scanning prior to deployment and during major updates. Reviews must follow recognized frameworks (e.g., OWASP, NIST) and address risks such as injection flaws, insecure authentication, and data exposure.

3.1.4.3.2 AI systems must be kept up to date in terms of updates and upgrades and shall be maintained accordingly.

3.1.4.4 Data Privacy

3.1.4.4.1 All AI systems must implement privacy-by-design principles, ensuring that only the minimum necessary personal data is collected, processed, and retained. Data usage must be purpose-specific, legally justified, and aligned with informed consent and applicable healthcare data protection regulations (e.g., ADHICS, PDPL).

3.1.4.4.2 Personal health data used in AI systems must be protected through strong encryption (at rest and in transit), anonymization or pseudonymization techniques, and secure key management as required. These safeguards must be applied consistently across the AI lifecycle—from data ingestion and model training to deployment and archival—to prevent unauthorized access and preserve patient confidentiality. Production data shall not be used to train the model.

3.1.4.4.3 All AI systems must incorporate data anonymization, differential privacy, secure multi-party computation, and federate learning into system architectures to minimize data exposure, enable data minimization, and uphold user confidentiality throughout processing workflows.

3.1.4.5 Infrastructure Security and Sovereignty

3.1.4.5.1 The compute and storage infrastructure of AI systems for both active and disaster recovery sites must be situated within the UAE. Additionally, remote access for development and support teams should be exclusively from within the UAE.

3.1.4.5.2 AI systems must be hosted in segmented, access-controlled networks with hardened configurations that prevent unauthorized lateral movement and isolate sensitive components.

3.1.4.5.3 Intrusion detection systems and continuous performance and access monitoring must be in place, with centralized logging and alerting to identify, respond to, and investigate security incidents in a timely manner.

3.1.4.6 Physical Security

3.1.4.6.1 All AI-supporting facilities must enforce strict physical access controls and continuous video surveillance to prevent unauthorized entry and to monitor sensitive infrastructure.

3.1.4.6.2 AI hardware must be equipped with tamper-proof mechanisms and monitored for physical breaches, with all incidents logged and investigated to maintain operational integrity.

3.1.5 **Fairness and Equity:** AI systems must operate without bias, delivering equitable treatment and outcomes for all intended population, regardless of race, gender, age, socioeconomic status, disability, or other personal characteristics.

3.1.5.1 Bias Prevention, Detection and Mitigation

3.1.5.1.1 All training, validation, and test datasets must reflect the diversity of the target population in terms of age, gender, ethnicity, socioeconomic status, comorbidities, etc.

3.1.5.1.2 Regular data representativeness audit must be conducted at defined checkpoints and subgroup coverage gaps must be flagged.

3.1.5.1.3 Bias detection techniques must be implemented, and mitigation efforts must be traceable.

3.1.6 **Transparency and Explainability:** All healthcare AI systems must maintain complete transparency by documenting data provenance, model logic, and decision outputs; and by clearly disclosing when AI technologies influence clinical or operational decision-making processes. All deployed AI solutions must provide human-interpretable explanations tailored to clinicians, administrators, and patients, with a clear disclosure of input factors and reasoning pathways behind critical healthcare decisions.

3.1.6.1 Stakeholder Communication

3.1.6.1.1 All healthcare AI systems must include mechanisms to inform patients, clinicians, and relevant stakeholders when AI contributes to clinical or operational decisions, specifying its function, limitations, and intended outcomes.

3.1.6.1.2 Communication protocols shall be established to ensure stakeholders receive clear, accessible summaries of the AI system's role—using plain language, contextual relevance, and formats appropriate to diverse audiences.

3.1.6.1.3 Patients must be informed of their right to opt out of AI-driven services where applicable. Clear consent mechanisms must be in place to ensure informed decision-making and transparency.

3.1.6.2 Documentation and Traceability

3.1.6.2.1 AI systems must document data sources, including provenance, preprocessing methods, and known limitations.

3.1.6.2.2 Model architecture, training logic, and decision criteria must be recorded in technical documentation.

3.1.6.2.3 All systems must maintain end-to-end traceability logs of inputs, outputs, and version history to support audits and compliance related investigations.

3.1.6.3 Role Specific Explanations

3.1.6.3.1 AI systems must generate role-specific explanations based on the end user (clinician, administrator, or patient).

3.1.6.3.2 Clinician-facing interfaces should prioritize clinical relevance, such as diagnostic rationale, confidence levels, and suggested next steps.

3.1.6.3.3 Patient-facing outputs must be plain-language summaries using non-technical terminology aligned with health literacy standards.

3.1.7 **Accountability and Responsibility:** Each phase of the AI lifecycle must have clearly defined roles and responsibilities assigned to accountable individuals or teams. AI systems that influence clinical or administrative decisions must include mechanisms for human oversight, escalation, and intervention to safeguard patient safety, uphold public trust, and ensure accountability in the face of adverse outcomes or ethical concerns.

3.1.7.1 AI Lifecycle Accountability and Responsibilities

3.1.7.1.1 AI systems must have designated owners responsible for ensuring alignment with core principles, adherence to standards, and effective management of risks.

3.1.7.1.2 Specific individuals or teams must be assigned responsibility for:

3.1.7.1.2.1 Monitoring AI outputs and exceptions.

3.1.7.1.2.2 Reviewing flagged cases or override events.

3.1.7.1.2.3 Reporting adverse outcomes or ethical concerns to governance bodies.

3.1.7.1.3 All decisions, changes, updates, and interventions must be logged and traceable to a responsible party, with version-controlled documentation available for internal and external audits.

3.1.7.2 AI Outcomes Accountability and Responsibilities

3.1.7.2.1 AI systems that influence clinical or administrative decisions must include mechanisms for human oversight, escalation, and intervention to safeguard patient safety, uphold public trust, and ensure accountability in the face of adverse outcomes or ethical concerns.

3.1.7.2.2 Clinicians should retain ultimate decision-making authority in all AI-assisted healthcare scenarios.

3.1.7.2.3 Override mechanisms and audit trails must be embedded in AI systems to ensure traceability and human intervention.

3.1.8 **Sustainability in AI:** AI systems must be designed using energy-efficient models, modular components, and low-carbon infrastructure. Data practices must emphasize minimization, reuse, and privacy-preserving techniques that reduce processing overhead. Sustainability impact assessments must be conducted for all high-impact AI systems, with transparent reporting on energy usage, emissions, and hardware utilization.

3.1.8.1 Energy Efficient Designs

3.1.8.1.1 AI systems must be designed and deployed using energy-efficient architectures and optimized algorithms to minimize carbon emissions and resource consumption throughout the lifecycle.

3.1.8.1.2 The design and implementation of AI solutions must prioritize environmental sustainability by utilizing low-power, high-efficiency infrastructures and ensuring algorithmic processes are optimized to reduce energy usage and ecological impact at every stage—from development to deployment.

3.1.8.2 Eco-friendly Lifecycle

3.1.8.2.1 Modular Design AI systems should be built using modular components that are easy to upgrade, replace, or reconfigure. This enhances longevity and reduces the need to discard entire systems when only part of them become obsolete.

3.1.8.2.2 AI systems should retire through strategies that minimize electronic waste at end of life.

## 3.2 Data Management

3.2.1 **Data Sourcing:** Data must be sourced from validated systems, protected through privacy-first practices, and maintained with full traceability, lifecycle documentation, and regulatory compliance.

3.2.1.1 All data sets used in AI systems must be sourced from authenticated clinical, operational, or research-grade sources, with acquisition metadata preserved to ensure full provenance, accountability, and contextual integrity.

3.2.1.2 Data must be collected, stored, and processed under enforceable privacy safeguards—incorporating encryption, role-based access, consent protocols, and auditable change logs.

3.2.1.3 Every dataset must be mapped to a clearly defined AI task. No speculative or indefinite-purpose data collection is permitted. Use must align with consent scope, ethical approvals, and declared benefit pathways.

3.2.1.4 When sourcing data from third parties, the DoH and all relevant entities within the Abu Dhabi healthcare ecosystem must adhere to procurement and data sharing policies, standards, and processes. The Legal Affairs Office, or its equivalent, must conduct thorough due diligence for third parties providing personal health information or sensitive health data to ensure that their data collection practices comply with all relevant UAE laws, healthcare regulations, and DoH standards.

3.2.1.5 Open Data is subject to licensing terms that may restrict the entity's ability to use the data for commercial purposes. When sourcing Open Data, licenses must be reviewed by the Legal Affairs Office, or its equivalent, to ensure compliance with data sharing and usage restrictions.

3.2.1.6 Web scraping of health sector-related data should be avoided where possible. If necessary, the Legal Affairs Office, or its equivalent, must be engaged beforehand to ensure compliance with privacy laws and ethical considerations.

3.2.1.7 Patient data or any data derived from patient information can only be used as permitted by patient consent agreements, healthcare regulations, and DoH's policies, standards, and processes.

3.2.2 **Data Usage:** Data Users are required to transparently report use of relevant attributes and disclose any discrepancies between dataset purposes and intended use.

3.2.2.1 Data Users are required to report both explicit and implicit uses of relevant attributes during the AI lifecycle. This includes identifying whether these attributes were used as a feature, proxy, or label.

3.2.2.2 Data Users must report any limitations in the datasets used and their potential impact on the AI health technology's performance. This includes investigating whether these limitations vary across different groups, such as those with Attributes categorized as 'unknown,' 'prefer not to say,' or 'other'.

3.2.2.3 Data Users must report any differences between the intended purposes of the datasets used and the Intended Use. The implications of such discordance on the dataset's suitability for its role must be clearly stated.

3.2.3 **Data Quality:** Datasets used for AI systems for training, validation, testing and production must meet stringent quality criteria.

3.2.3.1 Data used for AI systems shall be

3.2.3.1.1 clinically validated through domain-expert review, adjudication protocols, or verified diagnostics.

3.2.3.1.2 statistically appropriate for the intended medical use case and aligned with best practices.

3.2.3.1.3 relevant, representative of the target patient population, and free of errors or biases that could lead to disparities in healthcare outcomes.

3.2.3.1.4 subject to appropriate data governance and ethical oversight.

3.2.3.2 Datasets must be free from missing values, duplication, schema conflicts, and bias-inducing anomalies.

3.2.3.3 Data quality must be continuously monitored through automated checks and stakeholder feedback loops post-deployment. Any deviation, drift, or degradation must trigger revalidation actions in accordance with ethical governance policies and clinical safety thresholds.

3.2.4 **Data Versioning:** Datasets must be uniquely versioned, securely archived, and traceable ensuring reproducibility, auditability, and direct linkage to model outputs and development workflows.

3.2.4.1 Each dataset version must be uniquely identified, archived in immutable storage, and linked to specific AI development phases to ensure traceability, reproducibility, and rollback capability.

3.2.4.2 Versioning must follow structured protocols, including semantic versioning, detailed change logs, and explicit linkage to downstream models, ensuring lifecycle integrity and audit readiness.

3.2.5 **Metadata:** Each dataset version shall be accompanied by comprehensive metadata and documentation detailing its source, structure, preprocessing steps, and annotations, and shall be managed through centralized registry systems to ensure traceability and governance.

3.2.5.1 All datasets used throughout the AI lifecycle must be accompanied by comprehensive documentation. This documentation should ensure that data can be traced and audited at any stage.

3.2.5.2 Comprehensive metadata must accompany all datasets, detailing acquisition sources, preprocessing steps, annotator roles, and intended use, stored within centralized governance registries for traceability and compliance.

3.2.5.3 Documentation must include structured artifacts like datasheets or data cards, capturing ethical considerations, limitations, and maintenance protocols to uphold transparency and regulatory alignment.

## 3.3 Risk Management

3.3.1 The DoH and Healthcare eco-system in Abu Dhabi shall adopt and implement risk management for AI systems and related assets. Risk Management shall be proactive, evidence-based, and ethically grounded, ensuring that all AI-enabled systems are designed, deployed, and monitored with controls that protect patient safety, uphold public trust, and reinforce systemic integrity.

**The Risk Management process is comprehensively described in DoH Risk Management Protocol.**

#### 3.3.1.1 Risk Assessment

3.3.1.1.1 Risk Assessment must be done for all AI systems and related assets.

3.3.1.1.2 Risks must be documented and tracked using Risk Register.

3.3.1.1.3 Owners must be assigned for each risk.

#### 3.3.1.2 Risk Evaluation and Treatment

3.3.1.2.1 Risk ratings must be assessed, and suitable controls should be put in place.

3.3.1.2.2 Post control implementation, residual risk must be determined, and appropriate treatment plans must be devised.

3.3.1.2.2.1 **Very High Risk -** If AI systems pose very high residual risks, such systems must be prohibited for deployment (Avoid).

3.3.1.2.2.2 **High Risk -** If AI systems pose High Risk, such systems must undergo conformity assessments both prior to and following deployment. These assessments shall be conducted in coordination with the DoH DDGO, ensuring compliance with applicable ethical standards and statutory requirements.

3.3.1.2.2.3 **Medium Risk -** AI systems classified as presenting limited risk shall be subject to applicable AI governance policies, standards, and risk reporting obligations. Safeguards shall be applied to manage and mitigate risks to acceptable level, considering the specific context and intended use of the system.

3.3.1.2.2.4 **Low and Very Low Risk -** AI systems assessed as posing minimal or no risk, shall be exempt from formal risk reporting requirements, nevertheless, shall be kept under monitoring for effectiveness of the controls.

#### 3.3.1.3 Risk Monitoring

3.3.1.3.1 Consistent and systematic evaluation of the treatment plan's progress must be conducted to ensure the effective execution of mitigation strategies.

3.3.1.3.2 Periodic monitoring and review of controls must be conducted to ensure they are appropriate and effective; and any changes within the environment have not impacted the control effectiveness.

#### 3.3.1.4 Risk Communication

3.3.1.4.1 A comprehensive risk assessment, ongoing mitigation efforts, and related reports must be communicated with all stakeholders including the DoH for all AI Systems.

## 3.4 AI Literacy

3.4.1 The DoH and healthcare ecosystem in Abu Dhabi shall develop and implement continuous AI literacy programs aimed at enhancing understanding and competency among staff. These programs will include regular refresher courses to reinforce foundational knowledge, acceptable usage of systems, ethical principles in AI, information on regulatory frameworks; and mechanisms to gather and incorporate stakeholder feedback.

#### 3.4.1.1 Training and Awareness

3.4.1.1.1 All personnel interacting with AI systems shall be trained in ethical principles and regulatory framework of AI.

3.4.1.1.2 AI literacy shall be tailored to stakeholder roles:

3.4.1.1.2.1 Clinicians: Understand AI-assisted diagnostics, limitations, and override protocols.

3.4.1.1.2.2 Data Scientists: Ensure bias mitigation, explainability, and clinical relevance.

3.4.1.1.2.3 Administrators: Monitor compliance, risk classification, and governance metrics.

3.4.1.1.3 Training must include case studies of AI failures and success in healthcare to foster contextual judgment.

#### 3.4.1.2 Operational Integration

3.4.1.2.1 All personnel must be guided in integrating AI into business workflows and decision-making processes.

3.4.1.2.2 Stakeholders shall be equipped to critically assess AI outputs, including confidence scores, limitations, and potential biases.

3.4.1.2.3 Staff must be trained to identify when AI use is appropriate and when human judgment should prevail.

3.4.1.2.4 Literacy metrics shall be tracked via dashboards to assess organizational readiness and maturity.

## 4. Key stakeholder Roles and Responsibilities

| Stakeholder Name | Stakeholder Key Role |
|---|---|
| DoH's Data and Digital Governance Office (DoH's DDGO) | - Develop, review, and update Responsible AI governance frameworks, standards, and guidelines in alignment with UAE Ministry of AI guidelines, DGE regulations, and data standards.<br>- Ensure that all AI solutions within the Abu Dhabi healthcare ecosystem undergo ethical data use checks.<br>- Establish mandatory KPI to monitor AI use across entities in the healthcare ecosystem and collect KPI data from those entities.<br>- Conduct audits and assessments to ensure ongoing compliance with AI governance standards. |
| Product Owner or equivalent | -Ensure the development of AI systems aligns with responsible AI standards, focusing on eliminating or reducing risks through design and development choices.<br>-Provide clear and comprehensive documentation of AI models, including data sources, algorithms, and intended use cases.<br>- Manages AI systems, monitors and reports on risk. |
| Digital Governance Specialist or equivalent | - Categorize AI risks and ensure effective risk management processes are followed.<br>- Ensure that comprehensive technical documentation is maintained throughout the AI lifecycle.<br>- Implement post-deployment monitoring and reporting processes for AI systems. |
| Data Users or equivalent | - Provide comprehensive documentation for datasets.<br>- Identify Contextualized Groups of Interest at risk of disparate outcomes and ensure appropriate dataset representation.<br>- Report usage of Relevant Attributes, including Features, proxies, or Labels.<br>- Evaluate and report AI performance for all identified groups and address any unexpected disparate outcomes.<br>- Document methods used to modify AI performance.<br>- Disclose dataset limitations and their impact on AI performance.<br>- Report discrepancies between dataset purposes and AI technology goals.<br>- Review pre-existing assessments and highlight any risks to at-risk groups.<br>- Manage and mitigate risks through documented strategies. |
| Data Scientist or equivalent | - Conduct testing of AI systems to assess risks, ensuring AI solutions meet intended performance standards and comply with healthcare and safety regulations.<br>- Perform detailed assessments of AI algorithms for robustness, fairness, and accuracy, and document testing metrics and logs for compliance purposes.<br>- Support the AI development lifecycle by providing technical input on data processing, algorithm development, and the integration of machine learning models. |
| Legal Affairs Sector | - Overview regulatory compliance to ensure the implementation of relevant laws, regulations and industry standards. |

## 5. Monitoring and Evaluation

5.1 The DoH and Healthcare eco-system in Abu Dhabi 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 entities 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, 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 Responsible Artificial Intelligence 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 | June-2025 | AI policy standard | https://www.doh.gov.ae/en/resources/policies |
| 2 | July-2025 | AI Risk Management V1.0 | https://www.doh.gov.ae/en/resources/policies |
| 3 | Jan 2022 | Circular USO/29/2022 Abu Dhabi Healthcare Sector Cyberlearning Program | https://www.doh.gov.ae/en/resources/Circulars |
| 4 | May 2024 | Abu Dhabi Healthcare Information and Cyber Security [ADHICS] Standard | https://www.doh.gov.ae/en/resources/standards |