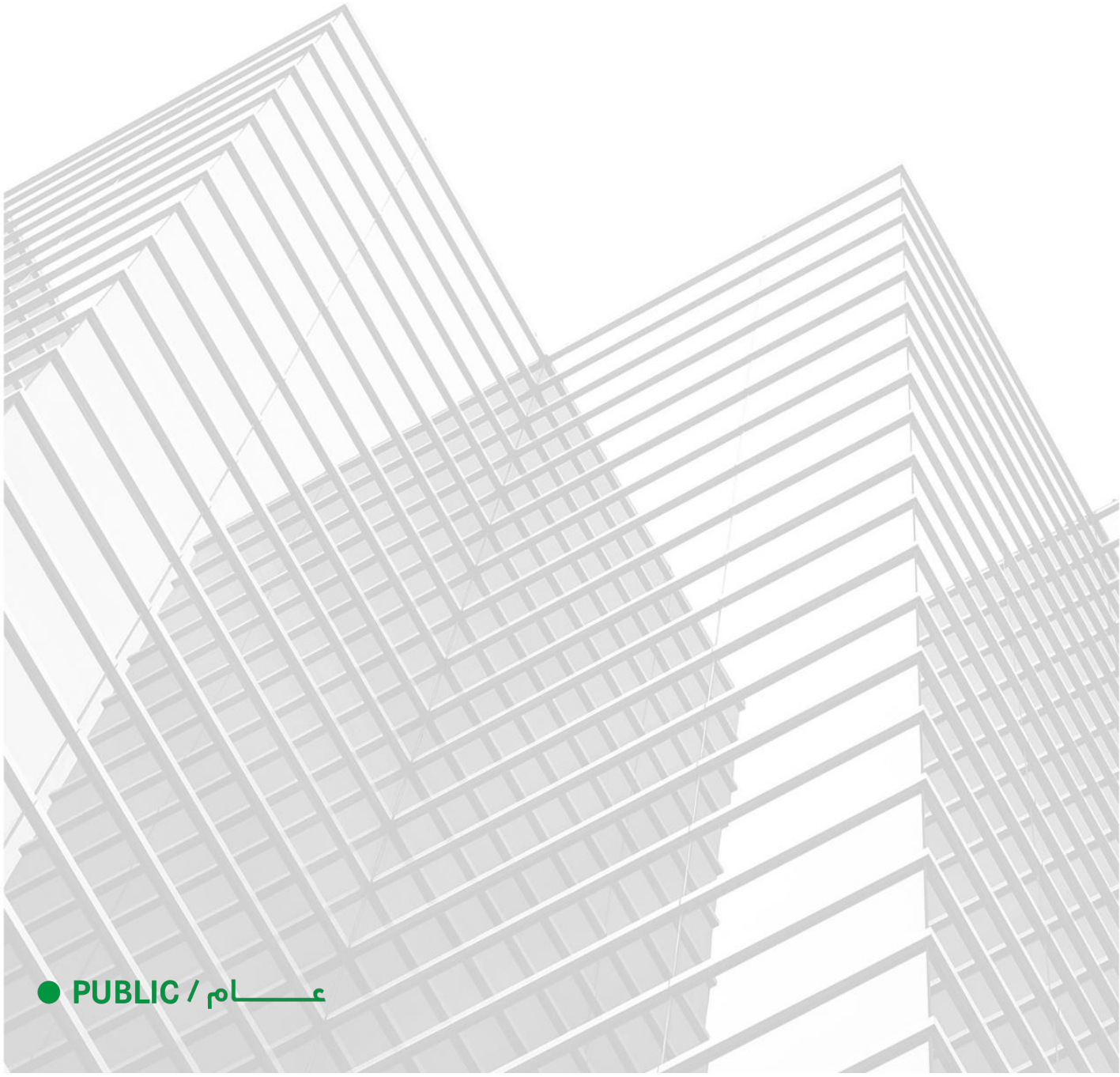
دائـــرة الـصـحـة
DEPARTMENT OF HEALTH

DIGITAL PRODUCTS GOVERNANCE STANDARD



PUBLIC / عـــــام

Document Title:	Digital Products Governance Standard		
Document Ref. Number:	DoH/ST/DHS/DPGS/V1/26	Version:	V1
New / Revised:	New		
Publication Date:	March 2026		
Effective Date:	Aug 2026		
Document Control:	DoH Strategy Sector		
Applies To:	All DoH stakeholders developing and managing digital products.		
Owner:	Data & Digital Governance Office		
Revision Date:	March 2029		
Revision Period:	Every three years		
Contact:	DDG@doh.gov.ae		

1.Standard Purpose and Brief

1.1 The purpose of the Digital Products Governance Standard is to establish a comprehensive framework for the effective management and oversight of digital products within the Abu Dhabi healthcare sector. This standard aims to ensure that digital products, including software, platforms, and technologies, are developed, deployed, and managed in a manner that adheres to regulatory requirements, and upholds the highest standards of quality, safety, and patient privacy. This standard aims to mitigate risks associated with patient privacy breaches, healthcare delivery disruptions, non-compliance with regulatory standards, and barriers to the creation and adoption of modern technologies, by setting strong and clear robust governance practices for digital products.

1.2 The successful implementation of this standard is expected to lead to the creation of a well-structured, transparent governance framework that enhances compliance with data protection regulations, encourages the development of high-quality digital products, fosters a culture of innovation, and facilitates continuous improvement in healthcare services.

1.3 Through this standard, the Department of Health (DoH) seeks to balance innovation with risk management, ensuring that digital health technologies contribute positively to the healthcare ecosystem in Abu Dhabi.

1.4 This Standard should be read in conjunction with the following guiding protocols

1.4.1 Annex A - Assign Digital Product Owner / Architect Protocol

1.4.2 Annex B - Digital Products Governance Feasibility Assessment Protocol

2.Definitions and Abbreviations

No.	Term / Abbreviation	Definition
2.1	Abu Dhabi Healthcare Eco-system	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	Data and Digital Governance Framework	A set of guidelines and principles established by the DoH to govern the collection, usage, and protection of data within the healthcare ecosystem.
2.3	Data and Digital Governance Office (DDGO)	A centralized unit within an entity 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 regulatory and legislative requirements with the organization's overall data and digital objectives.
2.4	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.
2.5	Digital Product Architect (DPA)	A professional responsible for designing and overseeing the technical architecture of digital products, ensuring they align with business objectives, regulatory requirements, and user needs while promoting scalability, security, and interoperability.
2.6	Digital Products	Refers to systems, applications, collaborative technology platforms, electronic health records, telemedicine, wearable devices that are powered by digital technologies such as robotics, IoT, 5G, Blockchain, Artificial Intelligence, Augmented Reality, Virtual Reality.
2.7	Digital Product Owner (DPO)	The DPO is responsible for the end-to-end management of digital products, including vision setting, stakeholder engagement, and ensuring alignment with entity's objectives and user needs.
2.8	Entity	Any organization, institution, or individual that operates within the healthcare ecosystem of Abu Dhabi and is subject to data governance regulations and standards mandated by DoH.

2.9	Patient	An individual receiving healthcare services, who owns their personal health information and provides consent for its usage as per data governance legislations and regulations.

3.Standard Content

3.1 Guiding Principles

To ensure a consistent and efficient approach to Digital Products Governance within Abu Dhabi's healthcare ecosystem, all entities and individuals involved shall adhere to the following principles:

Patient-Centricity: Design and operate digital products to enhance patient safety, privacy, and well-being, aiming to improve patient experiences and health outcomes.

Transparency: All stakeholders involved in the lifecycle of digital products shall maintain open communication and ensure all activities align with legal and ethical standards.

Security: All stakeholders shall strictly adhere to data protection laws, DoH Standards (including ADHICS V2) and implement best practices to safeguard patient information and enhance digital platform security.

Quality: All stakeholders developing and managing digital products shall commit to the highest standards of quality, ensuring reliability, effectiveness, and user-friendliness.

Innovation: All stakeholders shall cultivate innovation and agility in developing new products, enabling adaptability to changing healthcare environments.

Inclusion: All digital products shall be accessible and equitable, meeting the diverse needs of the population and ensuring inclusivity for all users.

3.2 Standard Statements

Outlined below are the fundamental standard statements governing the licensing, collection, usage, and protection of digital assets within the Abu Dhabi healthcare ecosystem.

3.2.1 Definition of Digital Products in Healthcare

3.2.1.1 Digital Product is defined as any software, application, platform, or technology developed and used within the healthcare sector of Abu Dhabi for purposes including but not limited to:

3.2.1.1.1 Collecting and managing patient information and healthcare records.

3.2.1.1.2 Facilitating communication between stakeholders in the healthcare ecosystem (patient, providers, payer, government).

3.2.1.1.3 Supporting clinical decision-making and healthcare service delivery.

3.2.1.1.4 Providing telehealth and remote healthcare services.

3.2.1.1.5 Offering educational resources for healthcare professionals and patients.

3.2.1.2 This definition encompasses products developed or utilized as healthcare solutions by the DoH, healthcare provider, technology company, or other entities operating within the Abu Dhabi healthcare ecosystem. Digital products can range from mobile applications to complex healthcare management systems and shall adhere to the regulatory standards established by the DoH.

3.2.2 Digital Products Governance Framework

3.2.2.1 DDGO or equivalent, shall establish and maintain a Digital Products Governance Framework. This framework aims to standardize and guide the development, deployment, and management of digital products across the entity.

3.2.2.2 All entities within the Abu Dhabi healthcare ecosystem shall adopt and align their digital products management practices with the standards developed by entities DDGO.

3.2.2.3 The Digital Governance Framework shall include detailed descriptions of digital governance bodies and roles, such as Product Owners, and Product Architects and Product Owners Working Group outlining their responsibilities, reporting structure, membership criteria, escalation hierarchy, and operational metrics.

3.2.2.4 Security standards should be established to protect digital products from cyber threats and ensure data integrity.

3.2.2.5 All entities within Abu Dhabi's healthcare ecosystem shall adhere to ethical practices in the development and management of digital products, ensuring the responsible use of technology. The DoH shall monitor compliance to ensure digital products are managed responsibly, respecting patient privacy, and adhering to consent protocols[1].

3.2.2.6 Documentation requirements shall be established to maintain records of product specifications, decisions, and governance activities.

3.2.2.7 All innovations shall strictly align with digital product governance principles and contribute to patient care quality, safety, and security.

3.2.2.8 The Digital Products Governance Framework shall be reviewed and updated as needed engaging with relevant stakeholders to gather feedback, ensuring the framework remains effective and responsive to new challenges, technological advancements, and changes in legislative and Regulatory requirements.

3.2.2.9 All entities within the healthcare ecosystem shall acquire necessary licenses and approvals (including regulatory) for digital health products, ensuring compliance with digital trust regulations and government service standards, and seek assistance from licensed developers and operators as required.

3.2.2.10 All entities within the healthcare ecosystem shall develop and implement business continuity strategies for digital technologies, addressing cybersecurity, technical requirements, and resilience planning, ensuring continuous service availability.

3.2.3 Digital Products Governance Bodies

3.2.3.1 DOH shall establish a governing body to oversee the digital governance landscape. Responsibilities of this governing body include, but are not limited to:

3.2.3.1.1 Approving relevant standards, policies, and protocols and monitoring their effective implementation

3.2.3.1.2 Reviewing and validating healthcare Digital Products Strategy

3.2.3.1.3 Ensuring compliance with all legal and regulatory standards

3.2.3.1.4 Facilitating the resolution of non-compliance issues

3.2.3.2 Each digital product developed within the Abu Dhabi healthcare ecosystem shall have assigned at least a Digital Product Owner or equivalent and a Digital Products Architect or equivalent, to ensure that digital governance standards are met. These roles can either be dedicated or added to the existing responsibilities of an individual. They are accountable for ensuring that digital product governance aligns with the framework, guaranteeing accountability within their respective products.

3.2.3.3 The DDGO shall establish a Digital Products Owners Working Group who ensures all digital products comply with DoH digital governance standards and regulations. The Working Group shall be responsible for reviewing healthcare regulations, addressing compliance challenges, and ensuring that health data and digital technologies are managed and exchanged in alignment with the DoH's standards and regulatory requirements.

3.2.4 Digital Products Initiation & Production

3.2.4.1 A feasibility study and risk assessment shall be conducted before initiating any digital product, including but not limited to financial viability, technological requirements, and potential impacts on stakeholders. For products that are required to get reviewed by DoH, follow process for DoH ADHTAC approval and DoH Web and Mobile Application approval[2]

3.2.4.2 Relevant stakeholders (e.g., end-users, legal, IT, Information/Cyber Security) shall be engaged early in the initiation phase to ensure alignment, identify needs, and address potential issues.

3.2.4.3 Digital Product Owners should prioritize user-centered design and conduct regular quality assessments to enhance usability, performance, and overall experience.

3.2.4.4 Digital products shall undergo thorough and rigorous testing, at a minimum, for functionality, security, accuracy, reliability, and user privacy before launch, ensuring they meet established quality standards, maintain data privacy, and adhere to interoperability and accessibility guidelines. This testing is essential to ensure that all digital products adhere to established quality assurance and interoperability standards prior to their deployment.

3.2.4.5 Digital Product Architects shall implement strict measures to protect data confidentiality, ensuring that Personally Identifiable Information (PII) and Protected Health Information (PHI) are secured against unauthorized access, misuse, or exposure.

3.2.5 Digital Products Management

3.2.5.1 Regular vulnerability assessments, penetration testing, and threat monitoring shall be conducted to identify and address potential security weaknesses or risks in digital products. Detected vulnerabilities shall be promptly addressed according to established security protocols by the Information and Cyber Security team.

3.2.5.2 Technical requirements for digital products including availability, response rates, compatibility, security, scalability, data integrity, and capacity must be specified and adhered to.

3.2.5.3 Resources must be allocated effectively, leveraging interoperable standards to enhance the agility and efficiency of technology development and deployment.

3.2.5.4 Protocols and standards must be established to ensure interoperability[3] and shall follow designated governance procedures to maintain this interoperability across digital activities.

3.2.5.5 Strategies on cybersecurity threats affecting digital products must be developed outlining specific response actions and mitigation plans.

3.2.5.6 Strategies to mitigate natural disasters must be established and their impact on use of digital products must be analyzed.

3.2.5.7 Change and release management plans for digital products must be established supporting comprehensive assessment of business needs and evaluating the impact on operations.

3.2.6 Privacy Policy Requirements

3.2.6.1 All digital products that are either developed by DoH, marked by DoH for governmental use, or owned by DoH, shall integrate UAE Pass as the standardized federal access protocol for authentication and identity verification across all digital products requiring end-user access.

3.2.6.2 The DoH and all entities within the Abu Dhabi healthcare ecosystem that develop, deploy, or manage digital products shall:

3.2.6.2.1 Implement and maintain a Privacy Policy, ensuring it incorporates the protection and confidentiality of user data and adheres to all legislative, regulatory, and compliance requirements related to privacy, as mandated by relevant government entities including the DoH's Information Security policies.

3.2.6.2.2 Display Privacy Notice on their websites and applications, making it accessible at user registration points or before digital product download, and secure affirmative user consent, such as through an 'I Agree' checkbox, to ensure informed user consent.

3.2.6.2.3 Develop and publicize procedures for responding to security incidents or breaches involving personal data, including clear guidelines on how users can report privacy concerns and how breaches will be managed and resolved.

3.2.6.2.4 Provide clear instructions within their Privacy Policy on how users can opt out or withdraw consent for the use of their personal data, ensuring users can easily understand and exercise their right to privacy and data protection.

3.2.6.2.5 Must secure separate affirmative consent from users for specific purpose. This should be facilitated through a distinct mechanism, such as an additional 'I Agree' checkbox, clearly explaining the nature of the data sharing, the entities with whom the data will be shared, and the purposes of such sharing, ensuring users make an informed decision.

3.2.6.2.6 Maintain records of user consents for acceptance of the Privacy Policy, Terms and Conditions, and End-User License Agreement.

3.2.7 Ethical Considerations

3.2.7.1 DoH and all entities within the Abu Dhabi healthcare ecosystem shall adhere to ethical standards in the use of health data within artificial intelligence, big data analytics, and other related technologies, ensuring that these practices respect patient confidentiality, consent, and data integrity, in anticipation of detailed guidance provided in a separate dedicated standard on ethical use of health data.

3.2.7.2 DoH and all entities within the Abu Dhabi healthcare ecosystem offering downloadable digital products, a clear and detailed End-User License Agreement shall be established. This agreement

should include, at minimum:

3.2.7.2.1 Outlining the licensing terms, including the scope of use, copyright notices, and restrictions.

3.2.7.2.2 Clarifying that the software is provided under a license, not sold, and detail the terms under which this license is granted.

3.2.7.2.3 Provisions on termination, limitations of liability, and warranty disclaimers.

3.2.7.2.4 Presentation to users for acceptance before they download or install the product.

3.2.7.3 DoH and all entities within the Abu Dhabi healthcare ecosystem entity shall establish Terms and Conditions or Terms of Use or Service Agreements for the digital products they own. This document should, at minimum:

3.2.7.3.1 Define the scope of services, user responsibilities, and the rules of conduct within the digital platform.

3.2.7.3.2 Highlight governing laws specific to Abu Dhabi's jurisdiction and any applicable international laws.

3.2.7.3.3 Include clauses on user contributions, third-party links, intellectual property, acceptable use, and the process for addressing breaches of terms.

3.2.7.3.4 Be available to all users and require explicit acceptance prior to product use or service engagement.

3.2.8 Issue and Risk Management

3.2.8.1 DoH DDGO shall create a systematic process for identifying, assessing, escalating, tracking, and resolving issues and risks impacting digital product effectiveness, compliance, and performance within Abu Dhabi's healthcare ecosystem.

3.2.8.2 **Risk Management** shall be proactive, evidence-based, and ethically grounded, ensuring that all digital products are designed, deployed, and monitored with controls that protect patient safety, uphold public trust, and reinforce systemic integrity. DDG risks may include but are not limited to Strategic and Business Risks, Data and Information Risks, Compliance and Regulatory Risks, Data Security, Sovereignty and Privacy Risks, Ethical Risks, Third-Party and Vendor Risks, Interoperability and Integration Risks

3.2.8.2.1 Risk Assessment must be done for all digital products and related assets as well as documented and tracked using Risk Register with defined ownership

3.2.8.2.2 Risk ratings must be assessed, and suitable controls should be put in place. Post control implementation, residual risk must be determined, and appropriate treatment plans must be devised.

3.2.8.2.2.1 **Very High Risk -** Such products must be prohibited for deployment (Avoid).

3.2.8.2.2.2 **High Risk -** Such products 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.

3.2.8.2.2.3 **Medium Risk –** Such products must be subject to applicable 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.

3.2.8.2.2.4 **Low and Very Low Risk –** Such products are exempt from formal risk reporting requirements, nevertheless, shall be kept under monitoring for effectiveness of the controls.

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

3.2.8.2.4 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.

3.2.8.2.5 A comprehensive risk assessment, ongoing mitigation efforts, and related reports must be communicated with all stakeholders

3.2.8.3 DDGO shall maintain the Data and Digital Governance Issue Log according to the three-tier priority system. This classification shall guide the urgency of response actions and the allocation of resources necessary for resolution.

DDG issues may include but are not limited to Governance Structure Issues, Data Ownership & Custodianship Issues, Data Access & Sharing Issues, Data Quality & Accountability Issues, Interoperability & Standards Issues, Privacy & Consent Issues, Data Security and Sovereignty, Compliance & Monitoring Issues, Platform & Technology Issues, Resource & Capacity Issues

3.2.8.3.1 **High Priority:** In the event of a high-priority issue (Immediate threats to patient safety, data security, regulatory compliance, or critical services), the impacted DDGO or equivalent shall

initiate immediate and decisive action to mitigate the issue

3.2.8.3.2 **Medium Priority:** For medium-priority issues (Significant operational impact without immediate critical threat), the impacted DDGO or 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 internally or within the entity

3.2.8.3.3 **Low Priority:** Low-priority issues (Limited immediate impact addressable through normal processes) 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.

3.2.8.4 DDGO shall design an escalation hierarchy, with defined SLA, for raising data-related risks and issues through the centralized mechanism, ensuring effective management and resolution of such concerns within the healthcare ecosystem.

3.2.8.5 DoH DDGO shall act as mediator and final decision authority for digital governance disputes including data ownership/custodianship, access rights, interoperability standards, platform hosting, master data definitions, and compliance interpretation.

3.2.8.6 DDGO shall maintain a Digital Governance Register documenting all governance actions, decisions, issues, risks, disputes, and resolutions.

3.3 Change Management

3.3.1 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:

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 The DDGO 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
Digital and Data Governance Office	Establish and maintain a Digital Products Governance Framework. This framework aims to standardize and guide the development, deployment, and management of digital products across the entity.
	Establish a Digital Products Owners Working Group who ensures all digital products comply with DoH digital governance standards and regulations
	Document and track all data-related actions, decisions, issues, and resolutions of the digital governance-related bodies in a data and digital governance register to ensure transparency and accountability.
	Design an escalation hierarchy for raising data-related risks and issues through the centralized mechanism, ensuring effective management and resolution of such concerns within the healthcare ecosystem.
	Implement a tiered issue classification system within its data governance framework to prioritize issues based on severity.
	Maintain the Digital Governance Issue Log according to the three-tier priority system.
Digital Product Architect	Develop architectural blueprints for digital products, ensuring they align with business goals, user requirements, and technical standards.
	Ensure the product architecture complies with security, privacy, and regulatory standards, including data protection protocols.
	Identify and integrate emerging technologies to enhance product functionality and user experience.
	Design the product to support scalability, maintain high performance, and optimize resource efficiency.
	Conduct risk assessments to identify potential technical challenges and implement mitigation strategies.
	Maintain comprehensive architectural documentation to support development, compliance, and future enhancements.
	Work closely with Product Owners, developers, and stakeholders to translate business requirements into technical specifications.
Digital Product Owner	Lead cross-functional teams to drive innovation, collaboration, and continuous improvement of digital products that enhance healthcare services
	Manage product lifecycles end-to-end—defining vision, strategy, roadmaps, and priorities—while engaging stakeholders, gathering requirements, and tracking KPIs.
	Champion user-centric design and ensure technical feasibility by coordinating with architects, developers, and data teams.
	Maintain compliance with DoH standards, internal policies, and regulatory requirements for security, privacy, and PII/PHI protection.
	Oversee documentation, governance, and reporting, and manage launches, updates, monitoring, backward compatibility, and eventual decommissioning.
Digital Products Owners Working Group	Ensure all products adhere to DoH regulations, data privacy laws, and digital governance standards.
	Conduct regular risk assessments and feasibility studies to identify potential operational, financial, and compliance challenges.
Health Data/Product Owners Working Group(s)	Work with IT, clinical, and regulatory teams to align digital product strategies with organizational goals.
	Ensure data quality, integrity, and accuracy across all digital products, upholding governance standards.

5. Monitoring and Evaluation

The entity shall establish a robust monitoring system to track and evaluate compliance with the standard. 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 this standard in accordance with the disciplinary regulation of the Healthcare sector.

7. Relevant Reference Documents

No.	Reference Date	Reference Name	Relation Explanation / Coding / Publication Links
1	11/2024	Patient Consent Standard	https://www.doh.gov.ae/en/resources/standards
2	2022	Circular **USO/68/2022**	https://www.doh.gov.ae/en/resources/Circulars
3	11/2024	Data Sharing, Integration, and Interoperability Standard	https://www.doh.gov.ae/en/resources/standards
4	11/2024	Digital Products Governance Feasibility Assessment Protocol	https://www.doh.gov.ae/en/resources/standards
5	11/2024	Assign Digital Product Owner Architect Protocol	https://www.doh.gov.ae/en/resources/standards
6	11/2024	Data Classification Standard	https://www.doh.gov.ae/en/resources/standards