Standards for Human Genetic and Genomic Data and Information Governance

Version (1)

Issue date: 28/08/2025

Effective date: 28/11/2025

Health Informatics and Smart Health Department

Dubai Health Authority (2025)

ACKNOWLEDGMENT

The Health Informatics and Smart Health Department (HISHD) developed this Standard in collaboration with subject matter experts and would like to acknowledge and thank all members of the roster for their dedication toward improving quality, safety and ethical management of Data Subject/Patient data in the Emirate of Dubai.

Dubai Health Authority

TABLE OF CONTENTS

INTRODUCTION

Health Regulation Sector (HRS) forms an integral part of Dubai Health Authority (DHA) and is mandated by DHA Law No. (14) Of the year (2021) amending some clauses of law No. (6) Of 2018 pertaining to the Dubai Health Authority (DHA), to undertake several functions including but not limited to:

- Developing regulation, policy, standards, guidelines to improve quality and Data Subject/Patient safety and promote the growth and development of the health sector.
- Licensure and inspection of Healthcare Facilities as well as healthcare professionals and ensuring compliance to best practice.
- Governing the use of narcotics, controlled and semi-controlled medications.
- Strengthening health tourism and assuring ongoing growth.
- Assuring management of health informatics, e-health and promoting innovation.

The Standards for Human Genetic and Genomic Data and Information Governance aims to fulfil the following overarching Dubai Health Sector Strategy 2026:

- Pioneering Human-centered health system to promote safety, quality and care for Data Subject/Patients and their families.
- Become a global digital health hub.
- Foster healthcare education, research and innovation.

EXECUTIVE SUMMARY

The purpose of this document is to assure the use of proper governance for Genetic and Genomic Data and Information in Healthcare facilities in the Emirate of Dubai. The standards have been developed to align with the evolving UAE health information governance legislations and international best practice. This document should be read in conjunction with the other health information governance documents released by DHA:

- Policy for Health Data and Information Sharing
- Health Data Quality Policy
- Health Data Classification Policy
- Policy for Health Information Assets Management
- Policy for Health Data Protection and Confidentiality
- Standards for Consent and Access Control
- Incident Management and Breach Notification policy
- Authentication and Authorization policy
- Information Security standard
- Artificial Intelligence Policy
- Guideline for transition of EMR
- Clinical Data Coding & Terminology Standards

DEFINITIONS

Active Health Information Asset: The Health Information Asset (HIA) that are consulted or used on a routine basis. Routine functions may include activities such as release of information requests, revenue integrity audits, or quality reviews.

Aggregated, Anonymised Genetic/Genomic Data: Genetic/Genomic data can never be fully anonymised due to its identifying nature. The term "Anonymised Data" refers here to data that has personal identifiers removed, and is grouped in cohorts or subsets to eliminate individualised data access, and reduce risks of indirect identifiability due to specific or rare characteristics.

Anonymisation: Anonymised information does not identify an individual; and cannot be practically used to determine their identity. Anonymisation requires the removal of any direct identifier and quasi-identifiers (e.g. detail, or combination of details, that might enable identification, either by itself or when used with other available information). Effectively anonymised information (where the prospect of identifying individuals is remote), is not seen as personal data and therefore data protection rules do not apply. The anonymised information can be used or disclosed without the Data subject's/Patient`s consent, as the information cannot be used to identify a specific individual. However, the anonymisation must be done effectively, and neither the anonymisation process, nor the use of the anonymised information, should have any direct detrimental effect on any particular individual.

Biobank/Biorepository: Large collections of biological materials (biospecimens) held for health and medical research purposes. They contain relevant personal and health information (which should include health records, family history, lifestyle, and Genetics information).

Bioinformatics: The application of computational tools, databases, and statistics to collect, store and analyze biological, medical and health information.

Biospecimen: A sample of biological material, such as urine, blood, tissue, cells, DNA, RNA, or proteins. Biospecimens should be used for a laboratory test or stored in a biobank for future research.

Biotechnology: Technology that utilizes biological systems, living organisms or parts of them to develop or create different products.

Coverage (Sequencing): Sequencing quality measure expressed either in percentage or average coverage, which considers the number of reads aligned to a specific locus in a reference genome.

Data Access Committee: The Data Access Committee objectively and systematically reviews data access requests from Data Requestors, in accordance with UAE laws and DHA Genomics policies and standards. The Committee should include, but not be limited to: senior operational personnel, data stewards, data domain leads, bioinformatician(s), Data Subject/Patient representative(s), and/or invited members of the relevant Flagship(s) and additional expert advisors.

Data Custodian: The Data Custodian is responsible for the safe custody, aggregation and storage of data.

Data Donor: a research participant, whose data have been collected, held, used for the primary research purpose and potentially shared for secondary research use.

Data Steward: The role of the Data Steward is to manage, oversee and utilise the organisation's data governance processes to ensure fitness of data elements - both the content and metadata. For Australian Genomics: Australian Genomics Managing Director and Data Manager.

Data Sharing Agreement: A legal agreement between the Facility/facility (as the controller) and the requester to share information/data according to specific terms and conditions and consistent with the principles of data sharing.

De-Identified Health Information/Data: Any Health Information or Subject of care Data that is been scrubbed of important identifiers such as birth date, gender, address, and age. The de-identified data is usually anonymized (i.e. does not identify a subject of care and with respect to which there is no reasonable basis to believe that the information can be used to identify a subject of care) in accordance with the requirements of Applicable Laws.

Disaster recovery site: is a facility an organization can use to recover and restore its technology infrastructure and operations when its primary data center becomes unavailable.

Disease-oriented biobanks: Collection of disease-specific biospecimens, focused on a single type of tissue or biospecimens from different sources that are relevant to a particular disease, such as cancer.

Electronic Medical Record (also known as Electronic Health Record): A systematic collection of electronic health information of an individual in a digital format that conforms to nationally recognized interoperability standards and enables information to be used and shared over secure networks.

Encryption: The use of an algorithmic process to transform Data into a form in which there is a low probability of assigning meaning without use of a confidential process or key. This will prevent unauthorized access to/use of information.

Entity: Any Entity or institution within the Emirate of Dubai that provides health services to people, including: the areas of prevention, treatment, and recovery, whether owned or managed by a natural or legal person. It may also include providers of health insurance or health insurance services, third party claims administrators, or those managing insurance requirements/services; or electronic services in the health field, or any services directly or indirectly related to the application of the provisions of this Standard.

Explicit consent: is a specific type of consent where an individual is clearly and expressly asked to agree to a particular use of their data. It involves a direct and unambiguous action, such as signing a consent form or checking a box that is not pre-checked.

Facility: is a Health Facility licensed by DHA to provide medical services to individuals, including areas of prevention, treatment, and convalescence owned and managed by natural or corporate body.

Gene: Functional and physical unit of hereditary information composed of chains of nucleotide base pairs that contains information for encoding a protein or protein subunit.

Genetics: refers to the study of individual human genes and how specific traits or conditions are inherited from parents to offspring.

Genomics: describes the study of individual human entire genome (all of its genes and their interactions). Focuses on complex diseases like cancer, diabetes, and heart disease, which result from

the interaction of multiple genes and environmental factors. Genomics also includes research on gene expression, epigenetics, and personalized medicine.

Genetics data: Personal data relating to the inherited or acquired Genetics characteristics of a natural person which give unique information about physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

Genetic Screening: Medical examination through which a gene or several genes of a person or persons identified by name is analyzed, and Genetic Areas of the DNA determined by the purpose of the test are examined.

Genomic Screening: Medical examination through which a gene of a person or persons identified by name is analyzed, and Genetic Areas of the DNA determined by the purpose of the test are examined.

Genetic Scanning: Process by which Genetic analysis is carried out on a large scale that includes a group of individuals identified on the basis of one or more traits they have in common, and not on the basis of prior knowledge of their names, in accordance with what is decided by the body organizing or implementing the Genetic Scanning.

Genomic Scanning: Process by which Genetic analysis is carried out on a large scale that includes a group of individuals identified on the basis of one or more traits they have in common, and not on the basis of prior knowledge of their names, in accordance with what is decided by the body organizing or implementing the Genomic Scanning.

Gene Therapy: Therapeutic procedure based on gene modification with the aim of treating the disease, suspend the progression of the disease, or prevent it through medical techniques that work to:

- Replace the disease-causing gene with a healthy copy of the gene.
- Disable a gene that causes a disease that is not working properly.
- Introduce a new or modified gene into the body to help treat or prevent disease.

Health Facility: DHA licensed health facility that performs medical examinations on patients, diagnosing their diseases, treating or nursing them, admitting them for convalescence, or assuming any activity related to treatment or to rehabilitation after treatment, whether it is owned or managed by natural or juridical persons.

Health Information Exchange (HIE): is the electronic transmission of health data and information among healthcare facilities according to national standards. Electronic health information exchange (HIE) allows doctors, nurses, pharmacists, other healthcare providers and Data Subject/Patients to appropriately access and securely share a Data Subject/Patient's vital medical information electronically—improving the speed, quality, safety and cost of Data Subject/Patient care.

Health Information System (HIS): Systems that collect, store, and process Protected Health Information (PHI) regardless of the owner of the system; for example: Electronic Medical Record (EMR), Health Information Exchange (Nabidh), Claims Management system, Public health portals, Practice Management Software, Data Subject/Patient Portals, Remote Data Subject/Patient Monitoring (RPM) Also known as telehealth, Laboratory Information System (LIS).

Inactive Health Information Assets: The HIA that involve a Data Subject/patient who has not sought treatment for a period of five (5) years. These HIA must be retained for reference, or to meet the full retention requirement.

Identifier or Identifying Information: Information where the identity of an individual is apparent or can reasonably be ascertained by the holder of the information. Information that should directly, or indirectly, lead to identifying an individual from whom the samples and associated information are collected as a link (or multiple links) exists between the participant's personal Identifiers and the data.

Incidents: A security incident is an event that leads to a violation or imminent threat of violation of information security policies, acceptable use policies, or Facility`s security standard; and puts sensitive data at risk of exposure.

Incompetent Data Subject: Refers to the Data Subject/Data Subject/Patient who either lack the full legal capacity or have the full capacity, but unable to provide a Consent.

Encryption at rest: is encryption that is used to help protect data that is stored on a disk (including solid-state drives) or backup media.

Information security: The act of protecting information that may exist in any form, whether spoken, written, processed or transmitted electronically, etc. from unauthorized access, use, disclosure, disruption, modification or destruction, with the objective of ensuring business continuity and minimizing business risk.

Least privilege: is an information security concept which maintains that a user or Facility should only have access to the specific data, resources and applications needed to complete a required task.

Master Data Management (MDM): deals with managing the core, non-transactional data assets that are used across the enterprise. It focuses on the consistent and reliable management of core business data like customers, products, and employees, creating a single source of truth.

Metadata Management: deals with the data about data, including its structure, format, and meaning, enabling better data understanding and utilization.

Minor: Any person below eighteen (18) years of age.

NABIDH: A health information exchange platform by the Dubai Health Authority that connects public and private Healthcare Facilities in Dubai to securely exchange health information.

Reference Data Management (RDM): focuses on managing and governing relatively static data sets used for classification, categorization, and cross-referencing within an organization.

Secondary Use of Health Information: is use of personal health information for purposes other than treating the individual subject of care, including but not limited to Research, Public Health, Quality Improvement, Safety Initiatives, payment and marketing. Some secondary uses directly complement the needs of primary use. Examples include medical billing, hospital administrative, and management operations.

ABBREVIATIONS

DESC	:	Dubai Electronic Security Centre
DHA	:	Dubai Health Authority
EID	:	Emirates Identity Document
EMR	:	Electronic Medical Record
GCC	:	Gulf Cooperation Council
HIE	:	Health Information Exchange
HIS	:	Health Information System
HISHD	:	Health Informatics and Smart health Department
ICT	:	Information and Communications Technology
IG	:	Information Governance
ISR	:	Information Security Regulation
IT	:	Information Technology
LIS	:	Laboratory Information System
MDM	:	Master Data Management
PHI	:	Protected/Personal Health Information
RDM	:	Reference Data Management
UAE	:	The United Arab Emirates.

1. BACKGROUND

Dubai Health Authority (DHA) is mandated by Local Law (6) of 2018 Concerning Dubai Health Authority and Local Law No. (14) Of 2021 on amending the local Law No. (6) of 2018 concerning the Dubai Health Authority to undertake several functions including, but not limited to Developing regulation, policy, standards, guidelines to improve and promote the growth and development of the health sector in the Emirate of Dubai.

The Standards for Human Genetic and Genomic Data and Information Governance aims to fulfil health information governance requirements for the management of Genetic and Genomic data and information. We hope this governance will enhance health-related data sharing and foster collaboration in genetic research, positioning Dubai as a leading global medical destination by establishing a value-based, comprehensive, integrated, and high-quality healthcare system.

2. SCOPE

2.1. All human Genetic and Genomic data and information that is generated, accessed, processed, stored, or shared within healthcare facilities operating under the jurisdiction of the DHA in the Emirate of Dubai.

3. PURPOSE

3.1. To establish and implement robust and ethical governance for human Genetic and Genomic data and information, ensuring compliance with the United Arab Emirates

(UAE) laws, Emirate of Dubai legislations, and DHA regulatory framework; while maintaining privacy, personal data protection, and Data Subject/Patient confidentiality.

3.2. To ensure lawful and appropriate use and responsible stewardship of human Genetic and Genomic data and information.

3.3. To safeguard and uphold the rights, welfare, and interests of Data Subjects/Patients regarding the access, sharing, processing, and storage of their Genetic and Genomic data and information.

4. APPLICABILITY

4.1. This Standard is intended for all DHA licenced Facilities, and Entities/individuals providing, storing, accessing, managing or otherwise using Genetic and Genomic related data, including data donors, users, and producers. This includes, but is not limited to, healthcare providers, researchers, research participants, research publishers, research funding agencies, data protection authorities, research ethics committees, research industry, providers of health insurance or health insurance services, third party claims administrators, or those managing insurance requirements/services; or electronic/digital services in the health field, or any services directly or indirectly related to the application of the provisions of this standard.

5. **STANDARD ONE:** PRINCIPLES OF GENETIC AND GENOMIC DATA GOVERNANCE

5.1. Facilities must implement robust ethical guidelines that prioritize Genetic and Genomic data confidentiality, integrity, availability, and respect for individual rights and cultural values.

5.2. Facilities must uphold the integrity and reliability of Genetic and Genomic data by implementing a strong data governance framework, supported by clear policies, standards, procedures, and defined Role-Based Access Control to ensure secure and effective data management.

5.3. Facilities must establish feedback mechanisms to assess the accuracy, quality, security, and efficacy of Genetic and Genomic data, along with their annotations, aiming to enhance data quality, promote interoperability, and support appropriate reuse by other relevant parties.

5.4. Facilities must store and process the Genetic and Genomic data they are collecting, using and transferring in a way that ensures accuracy, verifiability, fairness, objectivity, and up-to-date records. This approach supports data interoperability, reproducibility, and safeguards long-term accessibility and integrity.

5.5. Facilities must endorse harmonization of Genetic and Genomic data quality, confidentiality, security, management, retention, and access control.

5.6. Facilities must implement appropriate security measures that effectively eliminate the risk of unauthorized data access, alterations, loss, misuse, or destruction.

5.7. Facilities must maintain the flexibility to adjust the sensitivity level of Genetics and Genomics data through their Health Information Systems (HIS). Comply with applicable privacy and data protection regulations at every stage of data sharing and be in a position to provide assurances to Data Subjects/Patients that confidentiality and privacy are appropriately protected when data are collected, stored, accessed, processed, and exchanged.

5.8. Facilities must ensure privacy and data protection safeguards are appropriately aligned with the type and intended use of the Genetic and Genomic data, whether it is identifiable, coded or anonymized.

5.9. Facilities must ensure cybersecurity strategies are mandated for all HIS, platforms and softwares utilized in the storage and analysis of Genetic and Genomic data.

5.10. Facilities must ensure the long-term sustainability of generated Genetic and Genomic data by implementing proper archiving practices and utilizing suitable identification and retrieval systems. Furthermore, they should critically evaluate the tools and systems used for data retention.

5.11. Facilities should adopt DHA-recommended data integration and interoperability standards, including standardized data formats, protocols, and interfaces, to ensure seamless data flow/exchange across various HIS.

5.12. Facilities must ensure quality of Genetic and Genomic data by validating it for accuracy, consistency, and completeness. It is recommended to adopt specialized tools and procedures to support ongoing monitoring and continuous enhancement of data quality.

5.13. Data storage and operations within the Facility should encompass routine practices that ensure the accuracy, security, and accessibility of data. These processes must include data backup and recovery, security measures, and performance management as essential components.

5.14. Facilities should embrace document and content management systems that support the creation, editing, distribution, storage, and proper disposition of data.

5.15. Facilities should implement Reference Data Management (RDM) and Master Data Management (MDM) practices to ensure data is organized, archived, analyzed, and interpreted in a way that supports effective reporting and business analysis.

5.16. Facilities are recommended to implement Metadata Management to cover all aspects of metadata, including its definition, utilization, and ongoing management.

5.17. Facilities are recommended to establish a data warehousing strategy that enables business intelligence by delivering a centralized, organized, unified, and refined data repository to support fast and accurate information retrieval.

5.18. Facilities are recommended to adopt Big Data and Data Science practices, utilizing advanced data processing methods, predictive analytics, and real-time data analysis, supported by the establishment of a specialized data science team.

5.19. Facilities are required to conduct regular Data Management and Maturity Assessment to identify areas of strength and areas needing improvement in their data management practices.

5.20. A "Data Access Committee" should be established at the DHA level to oversee and regulate all matters related to the access and sharing of Genetic and Genomic data and information.

5.21. Sharing Genetic and Genomic data and information should be as per UAE laws and DHA Policy for Health Data and Information Sharing .

6. **STANDARD TWO:** CLASSIFICATION of GENETIC AND GENOMIC DATA AND INFORMATION

6.1. Facilities must classify Genetics and Genomic data and information as "Sensitive Data" in accordance with DHA Health Data Classification Policy.

6.2. Facilities must use appropriate codes for Genetic and Genomic data and information within their HIS as per Clinical Data Coding & Terminology Standards.

6.3. Facilities must use HIS that have the capability to "flag" sensitive data, as per the Health Data Quality Policy .

6.4. Genetic and Genomic data are more vulnerable than other identifiable data and require additional protection, breaches of the confidentiality must lead to regulatory investigation and should result in disciplinary measures to those who have been negligent in causing the breach as outlined in the Policy for Health Data Protection and Confidentiality.

7. **STANDARD THREE:** QUALITY of GENETIC AND GENOMIC DATA AND INFORMATION

7.1. Facilities must implement measures that comply with UAE laws and DHA regulations concerning data quality requirements including DHA Health Data Quality Policy .

7.2. Facilities must establish robust Information Technology (IT) infrastructure to minimize data quality issues, ensuring correct health information, demographic data, and Genetic and Genomic data are recorded and maintained.

7.3. Facilities must refine Genetic and Genomic data to eliminate duplicates, inaccuracies, incompleteness, and inconsistencies in the format.

7.4. Facilities must ensure that mandatory fields for Emirates ID numbers and demographic information are included in their HIS with a standardized format to guarantee data accuracy as required by DHA legislations.

7.5. Facilities must implement IT systems to integrate Genetics and Genomics data with other existing HIS, such as biobanks and EMRs.

8. **STANDARD FOUR:** SECURITY, INTEGRITY AND CONFIDENTIALITY of GENETIC AND GENOMIC DATA AND INFORMATION

8.1. UAE laws prohibit discrimination by employers, insurers, and other third parties based on Genetic information they obtain about an individual; Data subjects/Patients who undergo Genetic testing have a right to have their information kept in confidence.

8.2. Genetic and Genomic data and information must be protected and kept secure through appropriate technical and organisational measures during its entire lifecycle including collection, storage, access, processing, analysis, and sharing.

8.3. All Genetic and Genomic data and information must be archived and stored in accordance with the Information Security Regulation (ISR) requirements set by the Dubai Electronic Security Center (DESC) and in compliance with ISR version 3 cybersecurity standards.

8.4. Privacy and security should be ensured by proper infrastructure and cyber-security strategies within the Facilities.

8.5. All Facilities and their third-party partners must comply with UAE laws, DHA regulations, and DESC cloud security policies, which mandate that all data, including backups and disaster recovery sites, be hosted within the UAE.

8.6. Data Subject/Patients have the right to be informed about how and why the Facility collects, processes, stores and sometimes discloses their personal identifiable and confidential information under UAE data protection law: The UAE Federal Law No. (45) of 2021 Regarding the Data Protection .

8.7. Physicians and other healthcare providers involved in conducting and interpreting Genetic tests, or maintaining patient records containing Genetic test results, have professional and ethical responsibilities to:

8.7.1. Maintain the confidentiality of the Data Subject/Patient's Genetic and Genomic data and information.

8.7.2. Release Data Subject/Patient's Genetic and Genomic data and information to third parties only with the Data Subject/Patient's explicit consent.

8.7.3. Decline to participate in Genetic or Genomic testing at the request of third parties (e.g., for research purposes, etc.) unless explicitly requested and consented to by the Data Subject/Patient.

8.8. Both facilities and any third parties that are accessing, processing, or archiving the Genetic and Genomic data and information must:

8.8.1. Conduct regular security audit and penetration testing on HIS storing Genetic and Genomic data and information.

8.8.2. Enforce the concept of least privilege for all access to Genetics and Genomics data and information, whether by internal personnel within the Facility or by external third-party partners.

8.8.3. Establish mechanisms for consent revocation, enabling Data Subjects/Patients to withdraw their consent at any time.

8.8.4. Mandate encryption at rest for all Genetic and Genomic data and information.

8.8.5. Define anonymization methods to ensure protection against unauthorized re-identification.

8.8.6. Mandate logging and monitoring of data access to identify and prevent unauthorized usage.

8.9. Facilities must prevent unauthorised or unlawful access/processing/sharing, accidental loss, destruction or damage of Genetic and Genomic data.

8.10. Facilities must maintain high security measures when operating on-premises.

8.11. Facilities must enforce and maintain physical control over on cloud-basis servers by establishing contractual Data Sharing Agreements (DSAs) with the respective service providers.

8.12. Facilities must conduct regular, up-to-date cybersecurity audits.

8.13. Facilities must adapt technologies that prohibit attacks on Genomics and Genetics data stored/archived.

8.14. Facilities are responsible for developing, implementing, and maintaining safeguards that are suitable for the volume of Genetic and Genomic data and information collected and processed, the scope and nature of the processing activities, available resources and identified risks. This includes the use of encryption and de-identification where applicable.

8.15. Facilities must implement Differential Privacy (DP) techniques to ensure that individuals cannot be re-identified from aggregated or anonymized datasets.

8.16. Facilities should refer to health information governance documents released by DHA Digital Health Regulations for required data and information protection framework.

8.17. Facilities must utilize blockchain-based logging and verification for Genetic and Genomic data transactions to ensure records are secure and tamper-proof.

8.18. Facilities must strictly prohibit any attempt to re-identify anonymized data unless explicitly permitted by law.

8.19. Facilities must establish data-sharing systems that comply with the mandates of the UAE laws and DHA policies.

8.20. Facilities must have mandatory multi-factor authentication (MFA) for all individuals accessing Genetic and Genomic databases.

8.21. Facilities must ensure the ability to track data access and/or exchanges back to their source to prevent all unauthorized access attempts.

9. **STANDARD FIVE:** STORAGE AND BACK UP of GENETIC AND GENOMIC DATA AND INFORMATION

9.1. Built-in data back up feature should be implemented in Facilties producing, storing, proccessing Genetic and Genomic data and information.

9.2. Facilities must ensure the long-term, secure storage of Genetic and Genomic data to enable historical tracking and follow-up, in alignment with the UAE laws and DHA requirments.

9.3. Genetic and Genomic data archives should have a high standard of quality curation as erroneous, damaged, and obsolete data would lead to incorrect conclusions.

9.4. Facilities must have sufficient required infrastructure to guarantee Long-term secure storage of Genetic and Genomic data.

9.5. Automated data backup systems should be implemented within the Facility, ensuring data is immediately backed up upon upload.

10. **STANDARD SIX:** RETENTION OF GENETIC AND GENOMIC DATA AND INFORMATION

10.1. Genetic and Genomic data and related samples must be retained as per the UAE laws and DHA regulations.

10.2. If a Facility is closing due to unpredictable reasons, then the health information assets (including Genetic and Genomic data and related samples) should be transferred to a custodian Facility as per DHA policies and Standards for Health Information Assets Management During Closure.

10.3. The Data Subject/Patient should be informed before transferring the Genetic and Genomic Data to another Facility.

11. **STANDARD SEVEN:** THE DATA SUBJECT RIGHTS ON GENETIC AND GENOMIC DATA AND INFORMATION

As per UAE Federal Data Protection law No. (45) of year 2021 and DHA Policy for Health Data Protection and Confidentiality; there are rights for Data Subjects/Patients in respect of their Protected Health Information (PHI) being used or processed that must be respected by all:

11.1. The right to consent before processing Data Subject`s/Patient`s PHI: Without prejudice to any applicable legislation; anyone who exchanges and circulates Data Subject/Patient information must ensure its confidentiality and not use it for non-health purposes, and without the written consent of the Data Subject/Patient.

11.2. The right to receive information on:

11.2.1. Type of PHI being processed.

11.2.2. The purpose of processing PHI.

11.2.3. The source and recipient Facilities that will process Data Subject`s/Patient`s PHI.

11.3. The right to restrict/discontinue PHI processing in situations being defined on articles (16, 17 & 18) of the UAE Data Protection Law of year 2021.

11.4. The right to be informed of security measures being considered while transferring the PHI between Facilities as per DHA Standards for Consent and Access Control.

11.5. The right to be informed on the process and timeline of storing/archiving the PHI.

11.6. The right to be informed whether any automated decision-making, including profiling has/will been undertaken on their PHI.

11.7. The right for selective disclosure of PHI to Facilities as deemed necessary. Exercising this right should not impede the Data Subject's existing rights to availing healthcare services.

11.8. The right to request the transfer of their PHI whenever it is possible from technical aspects.

11.9. The right to request correcting any inaccuracies in their PHI, and have incomplete PHI to be fully completed. These requests must be assessed and responded by the Facility within 5 working days.

11.10. The right to be informed on Facility`s breach process; and how the Data Subject/Patient will be informed about PHI breach as per the UAE laws and DHA regulations.

11.11. Without prejudice to the applicable laws and legislations, and necessities of the public interest, the Data Subject/Patient has the right to request "opt-out" from the data and health information processing in conditions being defined on article (15) of the UAE Data Protection Law of year 2021 and DHA Standards for Consent and Access Control.

11.12. The right to access their PHI via "Subject Access Request" (SAR) and to review and obtain a copy of their PHI / records such as provider's medical and billing records or a health plan's enrolment, payment, claims adjudication, and medical management records maintained by the concerned Facility. The Facility must:

11.12.1. Document the verbal or written SARs with the signature of the Data Subject/ Patient.

11.12.2. Respond to the SAR within one month (e.g. 30 calendar days) of its receipt.

11.12.3. Ensure to update the HIS when accommodating these requests as and when needed.

11.12.4. Retain communications and documentations associated with these requests for a period mandated by the UAE Federal Law No. (2) of 2019 on the use of Information and Communications Technology in Health Fields and DHA requirements.

11.13. The right to lodge a complaint to the supervisory authority (e.g. DHA).

12. **STANDARD EIGHT:** EXPLICIT CONSENT FOR PARTICIPATING IN VOLUNTARY GENOMIC OR GENETIC SCREENING, SCANNING, OR RESEARCH

12.1. Explicit Consent should be taken from the Data Subject/Patient participating in the voluntary Genomic or Genetic screening, scanning, or research.

12.2. If the Data Subject/Patient is a minor (e.g. child/young person less than 18 years of age); the consent must be obtained from a person with parental responsibility/ or other legal guardianship for the minor. This authority must be verified and documented with the consent.

12.3. If the Data Subject/Patient is an incompetent or is unable to give the consent (e.g. mental or cognitive impairment: dementia, intellectual disabilities, or severe mental illness that prevent understanding and judgment; medical incapacity: unconscious or coma), it must be obtained from the next of kin (e.g. relatives up to the forth degree) or a person with legal guardianship. This authority must be verified and documented with the consent as per DHA Standards for Consent and Access Control .

12.4. The Data Subject/Patient or their legal representative/guardian must be fully informed about the screening, scanning, or research, ensuring they clearly understand its purpose and potential implications.

12.5. Consent should be specific, freely given, informed and unambiguous; using clear and plain language that is understood by the Data Subject/Patient.

12.6. Consent should be given in writing either in Arabic or in English.

13. **STANDARD NINE**: ACCESS TO GENETIC AND GENOMIC DATA AND INFORMATION

13.1. To the extent, technologically feasible users should be granted access only to Genetic and Genomic data required to carry out their designated responsibilities within the Facility.

13.2. Access must be restricted to specific functions within some applications; and whenever the software allows, access should be as granular as feasible.

13.3. Each user in the Facility should sign a "User and Confidentiality Access Agreement" before accessing Genetic and Genomic data.

13.4. Facility must issue passwords and Unique User Identification ("ID") for accessing Genetic and Genomic data once the "User and Confidentiality Access Agreement" is completed and submitted. Such passwords and IDs should not be shared with any other individuals or Facilities.

13.5. In configuring access, right to use should be granted on need-to-know basis and least privileges. Every user of the HIS should operate using the least set of privileges necessary to complete their job. This principle limits the damage that can result from data breach.

13.6. Facility must determine the specific functions and responsibilities for which the individual needs access for Genetic and Genomic data. The sensitive nature of many restricted functions, and their potential for abuse and error, should be considered when making this determination.

13.7. For healthcare providers, the role should be defined by the code associated with the license in Sheryan ID as maintained by DHA.

13.8. For employees who do not have Sheryan ID, the role should reflect one of the standard roles identified by HIS as determined by the Facility.

13.9. For Remote access to HIS, it is recommended to have additional authentication mechanisms, such as two-factor or hardware-backed certificates, to be deployed to individually authenticate and authorise all remote access to all networks and information systems that support staff`s essential service.

13.10. Access to Genetic and Genomic data should be granted with approval from the User's Director/Manager and approval from the system owner.

13.11. Access to Genetic and Genomic data and any related restricted applications, functions, and/or data sets should always be limited to those that are required for the performance of an individual's current duties.

13.12. Whenever the individual's duties at the Facility change, the individual's access to Genetic and Genomic data should also be changed to reflect this.

13.13. Authorization for access Genetic and Genomic data should be reviewed and validated regularly (at least every year along with the staff reappointment process).

13.14. Facilities must understand the issues related to lawful requests for Genetic and Genomic data; based on law enforcement, public health, or national security concerns.

14. **STANDARD TEN:** TRANSFER OF GENETIC AND GENOMIC DATA AND INFORMATION TO OUTSIDE THE UAE

14.1. Genetic and Genomic data and information are considered Protected Health Information (PHI) and should not be transferred to a country or territory outside the UAE as per UAE Federal Decree Law No. (49) of 2023 Concerning Regulating the Use of the Human Genome; except in cases specified by the UAE Ministry of Health and Prevention or DHA.

14.2. In these exceptional cases prior approval from DHA must be obtained in accordance with Policy for Health Information Sharing.

14.3. The approval can be granted by sending request to : HISH@dha.gov.ae

14.4. Any transfer or sharing of Genetic and Genomic data and information to outside of UAE must be carried out securely and safely to prevent the risk of accidental disclosure or loss in transit.

14.5. Genetic and Genomic data and information must be securely encrypted during transit; and all security measures outlined in UAE laws and DHA regulations must be strictly abide to.

15. **STANDARD ELEVEN:** SHARING GENETIC AND GENOMIC DATA AND INFORMATION

As per UAE Federal Decree Law No. (49) of 2023 Concerning Regulating the Use of the Human Genome:

15.1. All Genomic and Genetic data and information in the UAE must be completely maintained confidential and should not be circulated or disclosed except in cases permitted by the legislation in force in the UAE.

15.2. No Genomic and Genetic data and information should be used in a way that leads to discrimination between members of the community because of their Genetic traits or because of their ethnic origins or lineage which results in limiting their rights assigned to them under the legislation in force in the UAE.

15.3. No research or studies that include data, information, or statistics related to the UAE Genome Programme should be published, except after the approval of the UAE Minister of Health and Prevention or the Head of the Dubai Health Authority in accordance with the controls determined by the UAE Cabinet Resolution.

15.4. A National Genomic Database should be established in which Genomic and Genetic Data and Information should be stored accordingly. The UAE Cabinet Resolution will specify the Facility that should establish it, the sources of this data and information, the controls and procedures for registering and preserving it, managing it, using it, circulating and exchanging it, and the mechanisms for linking it to the relevant databases in all health, research and private bodies.

15.5. All concerned parties are obliged to provide the Facility, that is determined by the UAE Cabinet Resolution, with any Genomic and Genetic Data and Information available to them or to their affiliated facilities.

15.6. All parties organising or implementing a Genomic/Genetics Screening or Scanning for any purpose should provide the Facility determined by the UAE Cabinet Resolution with all Genomic and Genetics Data and information to be stored in the National Genomic Database.

15.7. In situations that there are victims of crises and disasters, or unknown persons whose DNA Profiling do not match any other DNA Profiling in the Federal DNA Profiling Database at the UAE Ministry of Interior; the Ministry of Interior or local police general commands should be granted the authority to view and exchange the data and information of those DNA Profiling with the National Genomic Database in accordance with the controls issued by the UAE Cabinet Resolution.

15.8. Sharing Genetic and Genomic data and information should be as per UAE laws and DHA Policy for Health Data and Information Sharing.

15.9. All sharing of Genetic and Genomic data and information with third parties must adhere to the following:

15.9.1. A legally binding and comprehensive "Data Sharing Agreement" must be in place, as outlined in the DHA Policy for Health Data and Information Sharing.

15.9.2. The third party (whether service provider, data processor, researcher, etc.) must undergo a thorough security assessment in accordance with ISR version 3 and Dubai Electronic Security Centre requirements.

15.10. Explicit consent must be obtained from the Data Subject/Patient for any purpose where no other legal basis for disclosure of Genetic and Genomic data and information can be identified.

16. STANDARD TWELVE: GENETIC AND GENOMIC DATA AND INFORMATION DISCLOSURES TO BLOOD RELATIVES

16.1. Data Subject/Patient`s Genetic and Genomic data and information may be vital for blood relatives for managing their medical/health condition.

16.2. Most Data Subject/Patients will readily share Genetic and Genomic information with relatives to assist those relatives with actual or potential health problems.

16.3. Healthcare providers should routinely discuss with Data Subjects/Patients the importance of family communication about Genetic findings and help them to identify the relatives that might need the information for screening and disease prevention purposes. During this discussion, healthcare providers might identify particular Data Subject/Patients who have difficulty in sharing their results with certain relatives and offer them targeted support.

16.4. It is important to highlight that both positive test results (indicating the presence of a Genetic basis for a disease) and negative test results (indicating no genetic link) have implications for the risk assessment of relatives and should be explained and discussed accordingly.

16.5. Although it is rare for individuals to completely refuse sharing important information with at-risk relatives, but where it happens, the healthcare provider should take time to consider whether alternative ways of disclosure are necessary. They should also assess the best approach to inform at-risk relatives, including if and when it may be appropriate to share Genetic/Genomic information. If a Data Subject/Patient declines to provide consent for disclosing their Genetic/Genomic condition to a blood relative, guidance should be obtained from the DHA 'Data Access Committee' to determine the appropriate course of action on a case-by-case basis.

16.6. Healthcare providers are responsible for notifying Parents/Guardians about abnormal Newborn screening test results and the need for secondary/or confirmatory testing and follow up, including referral to a specialist healthcare provider.

17. **STANDARD THIRTEEN:** SECONDARY USE OF GENETIC AND GENOMIC DATA

17.1. If Genetic and Genomic data and information is to be used for secondary purposes (e.g. purposes other than treating the Data Subject/Patient such as research, public health mandates, etc.), it is necessary to identify both a lawful basis for this usage and an additional condition for processing this type of data.

17.2. Below are list of some conditions for use of Genetic and Genomic Data and information for secondary use:

17.2.1. Employment purposes

17.2.2. Legal defense

17.2.3. Provision of Health Care

17.2.4. Public Health

17.2.5. Research

17.2.6. Statistical purposes

17.3. If disclosure to a competent public authority (e.g. public security or public health) is necessary to prevent serious crime or risk of serious harm; then Data Subject/Patient consent is not required.

17.4. Consent is not required if the data is anonymized and utilized exclusively for statistical purposes.

17.5. For research involving identifiable data, patient consent is mandatory.

18. **STANDARD FOURTEEN:** USING GENETIC AND GENOMIC DATA AND INFORMATION FOR INSURANCE SERVICES

As per article 20 of the UAE Federal Law by Decree No. (49) of 2023 Regulating the Use of the Human Genome:

18.1. Insurance Corporations should not enforce those seeking insurance coverage to a Genomic or Genetic Screening aimed at detecting and predicting their susceptibility to diseases and considering it as a basic requirement for providing insurance services to individuals.

18.2. Insurance Corporations should not request or use the results of any previous Genetic or Genomic Screening for those seeking insurance coverage.

19. **STANDARD FIFTEEN:** USING GENETIC AND GENOMIC DATA AND INFORMATION FOR SCIENTIFIC RESEARCH PURPOSES

19.1. The sources of Genetic and Genomic Data and information, the controls and procedures for registering and preserving, managing, using, circulating and exchanging this data, and the mechanisms for linking it to the relevant databases in all health HIS, research, and academic institutes, and private companies/vendors should be determined according to the UAE Cabinet Resolution for Federal Law by Decree No. (49) of 2023 Regulating the Use of the Human Genome .

19.2. Facilities must make reasonable efforts to enhance the accessibility/usage of Genetic and Genomic data for research purposes as per framework explained in the UAE law and DHA regulations.

19.3. Facilities must promote collaborative partnerships and data sharing that can generate maximum scientific and community benefit as per UAE law and DHA regulations.

19.4. Dissemination of Genetic/Genomic data and research results should be conducted in a way that promotes scientific collaboration, while minimizing harms and maximizing benefits to individuals, families and communities.

19.5. Scientific or clinical research related to the Human Genes and Genome must be carried out in accordance with the following controls:

19.5.1. Fulfilling the requirements and controls contained in the legislation regulating scientific and clinical research in the UAE.

19.5.2. Achieving scientific objectives related to the following:

a. Reviewing and understanding the structure and function of the human body.

b. Reviewing and understanding diseases that affect humans.

c. Promoting public health.

19.6. Human cloning or modifying the human traits of persons and embryos for purposes that violate the provisions of the UAE law, or that involve the risk of generating genetically modified biological organisms that pose a threat to humans and the environment is forbidden.

19.7. All diagnoses, results, data and information related to Genetic and Genomic data, which were carried out or arrived at within the framework of scientific or clinical research, must be kept completely confidential, and should not be disclosed except in cases permitted by the legislation in force in the UAE.

19.8. Facilities must develop procedures to identify and address conflicts of interest of researches accessing Genetic and Genomic data and information.

20. **STANDARD SIXTEEN:** TRAINING AND DOCUMENTATION of GENETIC AND GENOMIC DATA AND INFORMATION

20.1. Facilties must train all employees and workforce members (e.g. trainees, researchers, vendors, contractors and anyone over whom the Facility exercises direct control) on appropriate Genetic and Genomic data and information access, the terms in the “User and Confidentiality Agreement”, and it`s health information consent and access control

policy, as necessary and appropriate for them to carry out their functions; as per principles of this standard and Standards for Consent and Access Control

20.2. All Facility`s employees and workforce members should be trained on privacy and security protocols, as well as the specific procedures for managing Genetic and Genomic data and information to mitigate security risks.

20.3. Facilities must maintain comprehensive documentation of the entire Genetic and Genomic data and information governance; with ongoing training and regular updates to reflect changes in laws and technologies.

20.4. Facilities must allocate resources for education and training to enhance Genetic and Genomic data accessing, sharing and management, and to constantly improve data quality and integrity.

20.5. Education and training resources should also be dedicated to:

20.5.1. Promoting and maintaining accurate Genetic and Genomic data that will impact and outcomes of data sharing, public health studies, clinical research, and strategic decision making.

20.5.2. Raising awareness on national health priorities and the distribution of health services.

20.5.3. Strengthening capacity and infrastructure for Genetic and Genomic data sharing at the national level.

21. **STANDARD SEVENTEEN:** AUDIT AND MONITORING

21.1. Clinical Audit and Control Department in Dubai Health Authority will conduct regular inspection to audit on Genetic and Genomic data and information governance process within the Facility to ensure compliance with the established standards.

21.2. A failure to adhere to this standard is considered a violation that requires investigation. Disciplinary action/dismissal will be taken in accordance with the provision of the current UAE laws and DHA legislations.

21.3. Facilities must implement mechanisms for handling complaints related to data misuse, identifying, reporting, and managing breaches.

21.4. All related breached should be promptly investigated as per DHA Policy for Health Data Protection and Confidentiality

21.5. Health information and smart health department should be informed through email HISH@dha.gov.ae

21.6. Data Subjects/Patients who experience discrimination due to illegitimate access/usage of their Genetic/Genomic Data and information have rights to report the misconduct to Info@dha.gov.ae

REFERENCES

1. UAE Federal Law by Decree No. (49) of 2023 Regulating the Use of the Human Genome. Available on: https://www.dha.gov.ae/uploads/062024/Federal%20Law_49_2023_Regulating%20the %20Use%20of%20the%20Human%20Genome202466484.pdf
2. Australian Genomics Policy on Data Access and Sharing for Secondary Use. Available on: https://www.australianGenomics.org.au/wp-content/uploads/2021/05/Australian-Genomics_Data-Access-Policy_20220607.pdf
3. Guidelines for Clinical & Translational Research in Genomics. Available on: https://www.doh.gov.ae/-/media/Feature/Resources/Guidelines/Guidelines-for-Clinical-and-Translational-Research-in-Genomics.ashx
4. The Global Alliance for Genomics and Health (GA4GH). Available on: http://oicr.on.ca/oicr-programs-and-platforms/global-alliance-Genomics-and-health-ga4gh
5. Melbourne Genomics Health Alliance Governance of Genomic data. Available on: https://www.melbourneGenomics.org.au/about-us/our-work/project-portfolio/data-and-information/governance-Genomic-data
6. Royal College of Physicians and Royal College of Pathologists Consent and confidentiality in Genomic medicine report (3rd edition, 2019). Available on: https://bsgm.org.uk/media/11524/consent_confidentiality_working_report_final_online_2019.pdf

7. Comment on Informing relatives of their Genetic risk: an examination of the Belgian context. Aisling de Paor. European Journal of Human Genetics volume 30, pages749–751 (2022). Available on: https://www.nature.com/articles/s41431-022-01066-1

8. Standard of Biotechnology and Bioinformatics in Medical Genomics. Department of Health Abu Dhabi. Available on : https://www.doh.gov.ae/-/media/FAF5741F3D6A4E9E91C14390139BFC9D.ashx

9. UAE Federal Law No. (2) of 2019 On the Use of Information and Communications Technology (ICT) in Healthcare. Available on : https://www.dha.gov.ae/uploads/082022/Federal%20Law% 20No2022824434.pdf

10. Dubai government Information Security Regulation. Available on: https://www.desc.gov.ae/regulations/standards-policies/

11. UK Guidance on Genomics and Research in Sensitive Bioinformatics Data. available on: https://researchethics.dk/guidelines/guidance-on-Genomics-and-research-in-sensitive-bioinformatics-data

12. European Data Governance Act. Available on : https://www.european-data-governance-act.com/

13. Genomic Data Policy Framework and Ethical Tensions. Available on: https://www3.weforum.org/docs/WEF_Genomic_Data_Policy_and_Ethics_Framework_pages_2020.pdf

14. NHS Borders Information Governance Code of Conduct. Available on: https://www.nhsborders.scot.nhs.uk/media/878869/2021-08-18-information-governance-code-of-conduct-version-24_1.pdf

15. World Health Organization (WHO). Guidelines on the management of Genomic data in clinical settings. Available from: https://www.who.int

16. National Institutes of Health (NIH). Genomic data management in clinical settings: Guidelines and best practices. Available from: https://www.nih.gov

17. National Human Genome Research Institute (NHGRI). Managing Genomic data in healthcare: A clinical guidelines framework. Available from: https://www.genomeweb.com

18. European Society of Human Genetics. Ethical, legal and social aspects of Genetic testing and Explicit consent. Available from: https://www.eshg.org

19. American Medical Informatics Association (AMIA). Genomic data management and sharing in clinical practice: Guidelines for implementation. Available from: https://www.amia.org

20. Future-proofing Genomic data and consent management: a comprehensive review of technology innovations

21. Adrien Oliva, Anubhav Kaphle, Roc Reguant, Letitia M F Sng, Natalie A Twine, Yuwan Malakar, Anuradha Wickramarachchi, Marcel Keller, Thilina Ranbaduge, Eva K F Chan. GigaScience, Volume 13, 2024. Available on: https://doi.org/10.1093/gigascience/giae021

22. Framework for responsible sharing of genomic and health-related data. available on: https://www.ga4gh.org/framework/

23. Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (OECD 2013). Available on: https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/oecd_fips.pdf

24. Aaronson, S. A. (2019). Data is Different, and That's Why The World Needs A New Approach to Governing Cross-Border Data Flows. *Digital Policy, Regulation and Governance* , *21*(5). https://doi.org/10.1108/DPRG-03-2019-0021

25. Nisar, Q. A., Nasir, N., Jamshed, S., Naz, S., Ali, M., & Ali, S. (2020). Big Data Management and Environmental Performance: Role of Big Data Decision-Making Capabilities and Decision-Making Quality. Journal of Enterprise Information Management, 34(4). https://doi.org/10.1108/JEIM-04-2020-0137

26. Shepherd, E., Bunn, J., Flinn, A., Lomas, E., Sexton, A., Brimble, S., Chorley, K., Harrison, E., Lowry, J., & Page, J. (2019). Open Government Data: Critical Information Management Perspectives. *Records Management Journal*, *29*(1–2). https://doi.org/10.1108/RMJ-08-2018-0023

27. Wibisono, A., Sammon, D., & Heavin, C. (2022). Data Availability Issues: Decisions as Patterns of Action. Journal of Decision Systems, 31(S1). https://doi.org/10.1080/12460125.2022.2070945

28. Zhang, Q., Sun, X., & Zhang, M. (2022). Data Matters: A Strategic Action Framework for Data Governance. *Information and Management*, *59*(4). https://doi.org/10.1016/j.im.2022.103642

29. Zorrilla, M., & Yebenes, J. (2022). A Reference Framework for The Implementation of Data Governance Systems for Industry 4.0. *Computer Standards and Interfaces*, *81*. https://doi.org/10.1016/j.csi.2021.103595

30. Information security, cybersecurity and privacy protection – information security management systems – requirements, third edition. Geneva: International Organization for Standardization; 2022 (ISO/IEC 27001:2022; https://www.iso.org/standard/27001).

31. Information security, cybersecurity and privacy protection – information security management systems – requirements, third edition. Geneva: International Organization for Standardization; 2022 (ISO/IEC 27001:2022; https://www.iso.org/standard/27001).

32. Risk management. Geneva: International Organization for Standardization; 2018 (ISO 31000; https://www.iso.org/iso-31000-risk-management.html).

33. Guide for conducting risk assessments. Gaithersburg (MD): National Institute of Standards and Technology; 2020 (NIST SP 800-30 Rev. 1; https://doi.org/10.6028/NIST.SP.800-30r1).

34. Information security, cybersecurity and privacy protection – information security controls. Geneva: International Organization for Standardization; 2022 (ISO/IEC 27002:2022; https://www.iso.org/standard/75652.html).