

PRIVACY POLICY

I.2. GENERAL STATEMENT

We, Arabia Insurance Company S.A.L explain with this Privacy Policy how the customer's rights to privacy

is protected and respected as we stand by our commitment to treat your information responsibly.

This Policy describes and explains how Arabia Insurance Company may collect, use and share information from/about you.

I.3. Collecting Your Personal Information

We, Arabia Insurance Company collect personal information about you from different sources. For example, we collect information you submit to us on applications and forms. Arabia Insurance Company contracts with certain unaffiliated business partners who help us deliver products and services online, by Brokers or Third-Party Providers etc... who may keep the information you provide.

Arabia Insurance Company may also collect the information you provide when you:

- request information from one of Arabia Insurance Company's Websites
- use online tools and calculators
- apply online for products
- subscribe to online services
- complete an online form
- conduct transactions online

I.4. Using Your Personal Information

Arabia Insurance Company collects personal and confidential information in the normal course of business to provide services to clients. This information may be used:

- to communicate with you;
- to process your requests and ensure that the relationship with you is accurate and up-to-date;
- to respond to your inquiries;
- to send you important information regarding your relationship with Arabia Insurance Company, changes to the Privacy Policy, or any other administrative matter;
- to allow you to participate in surveys and promotions;
- for data analysis, audits, developing and enhancing the Company's products and services, and developing the site;
- for identifying usage trends and determining the effectiveness of promotional campaigns;
- for risk control, and fraud detection and prevention;
- to comply with laws and regulations;
- to send you marketing communications that may be of interest to you.
- If you also purchased a different financial or insurance product, we may share your information for marketing purposes.

I.5. Sharing Your Personal Information

We, Arabia Insurance Company may share your personal information with reinsurers, service providers and third parties that carry out services and marketing for us. We may share your information in whole or in parts as required or permitted by law, for a legal or regulatory purpose or to combat fraud. These include the following types of information:

- We may share information we receive from you on applications or other forms. This may include your name, address, beneficiaries, Social Security number, and family member information. This may also include assets, income, and the property address and value.
- We may share information from your transactions with our sister companies. This may include your account balance, policy coverage, and payment history. This may also include premium paid, preferences, claims, and purchase method.
- We may share information we receive from a consumer-reporting agency or other report. This may include your credit report, motor vehicle, and driver data. This may also include medical and employment data, loss history reports, and other driver data.
- We may share information concerning your mode of payment with authorized third parties. All credit/debit cards details and personally identifiable information will not be stored, sold, shared, rented or leased to any unauthorized third parties.

You will find a link to some of the entities allowed access to part or all of your confidential information for business reasons by Arabia Insurance Company:

- R+V Versicherung AG

With regard to the processing of your Personal Data as defined by the European General Data Protection Regulation (GDPR) by our European partners, you can find further information on the respective entities, in accordance with Article 14 GDPR, under:

- For R+V Versicherung AG, please access <http://www.gdpr.ruv.de>

I.6. Using Your Medical Information

Sometimes, we must collect medical information to provide you a product or to pay a claim. We use medical information when:

- Underwriting insurance
- Servicing your policy, account, or claim
- As required or permitted by law
- At your request and with your authorization

I.7. Information Accuracy

Personal and sensitive information should be as accurate, complete and up-to-date as necessary for its purpose of use. If you believe your information is inaccurate, incomplete or not current, please contact Arabia Insurance Company or your designated agent.

I.8. Confidentiality and Security

Personal and confidential information is protected by security safeguards matching the sensitivity of the information. Safeguards against loss, theft, unauthorized access, copying, use or modification is addressed, including physical security measures (locks, restricted access areas, etc.), organizational measures (security clearances, authorization processes, etc.) and technological measures (passwords, encryption, multifactor authentication, etc.). The nature of the safeguards matches the level of information sensitivity.

We use physical and technical safeguards to protect your information. We restrict access to your information to those who need it to perform their jobs. Third-party business partners are bound by law to use the information only for our purposes. They may not disclose it or use it in any other way. We comply with all data security laws.

Privacy Policy Updates and Changes

This Privacy Policy may be subject to change without prior notice. Changes to the Policy posted on the website will become effective immediately. Therefore, the Customers' are encouraged to frequently visit these sections in order to be updated about the changes on the website.



Website & Social Media

Platform Privacy Policy

Arabia Insurance Company may collect Information that does not reveal your explicit identity or does not directly relate to a person, such as information collected through cookies, browser information, and other technologies, demographic information and other information that you provide.

Arabia Insurance Company may collect and use information in a variety of ways, including but not limited to: **Browser, Cookies, IP Address, Combined Data.**

Arabia Insurance Company or our business partners use the information from our websites for many purposes:

- edits and feedback
- marketing and promotions
- analysis of user behavior
- product development
- content improvement
- informing advertisers how many visitors have seen or clicked on their advertisements
- customize Web site content and layout

II. Advertising

Arabia Insurance Company may advertise on its website as well as on other affiliated websites. Information collected by Arabia Insurance Company or its advertising service providers through cookies and other technologies includes the number of people who surf the site, browsing patterns within the site, and responses to advertisements and promotions on the site and on websites where the Company advertises.

Arabia Insurance Company may advertise products and services on this website, including offers of Policies. These advertisements may take the form of splash ads (ads that appear as you sign on or sign off of your online accounts), banner ads, etc.

Arabia Insurance Company also resorts to advertising service providers to be able to determine which advertisements are most likely to be of interest to you, using certain information such as web pages visited, search keywords entered, or your activities on the site. Arabia Insurance Company limits access and collection of information to specific purposes for advertising service providers.

III. Third Party Sites

Arabia Insurance Company may provide links to third party websites, such as reinsurers or service providers. If you follow links to websites not affiliated or controlled by Arabia Insurance Company, you should review their privacy and security policies and their terms and conditions, as they may be different from those of the Company's sites. Arabia Insurance Company is not responsible for and does not guarantee the security or privacy of these websites, including the completeness, accuracy, or reliability of the information published thereon.

Some of the advertisements you see on this Website are selected and delivered by third parties, such as ad networks, advertising agencies, advertisers, and audience segment providers. These third parties may collect information about you and your online activities, either on this Website or on other websites, through cookies, web beacons, and other technologies in an effort to understand your interest and deliver advertisements that are tailored to your interests. Please remember that we do not have access to, or control over, the information these third parties may collect. The information practices of these third parties are not covered by this privacy policy.

IV. Social Media

Arabia Insurance Company may use social media platforms including, but not limited to, Facebook, Twitter and LinkedIn to enable online sharing and collaboration among users. Any content you post on official Arabia Insurance Company managed social media pages, such as opinions, pictures, or any personal information that you make available to other participants on these social platforms, is subject to the Terms of Use and Privacy Policies of those respective platforms. Please refer to them to better understand your rights and obligations with regard to such content. In addition, please note that when visiting any official Arabia Insurance Company social media page, you are also subject to Arabia Insurance Company Privacy Policy.

General Disclaimer and Consent For eArabia

V. Disclaimer

By accessing, viewing, using, or downloading materials from E-Arabia, you indicate that you have read and understood this Policy and further agree to accept all information contained herein without limitation or qualification and to be legally bound by them. This Policy is applicable to your use of E-Arabia regardless of how you accessed it. IF YOU DO NOT AGREE TO BE LEGALLY BOUND BY THIS POLICY, YOU MUST DISCONTINUE USING AND EXIT E-Arabia IMMEDIATELY.

Arabia Insurance Company (“Arabia”) reserves the right, in its sole discretion, to modify or change this Policy at any time without prior notice. Your continued use of E-Arabia following the posting of any changes constitutes your acceptance of the then current Policy. If at any time, you choose not to accept this Policy, you are not authorized to use E-Arabia.

You may not use E-Arabia to engage in any illegal or fraudulent activities or conduct which is defamatory, libelous, threatening or harassing or that infringes on a third party’s intellectual property or other proprietary rights and Arabia Insurance Company shall be held harmless upon the commitment of such acts and shall not thereof be bound to cover or continue to cover the infringing User.

Statements on E-Arabia as to policies and coverages provide general information only. Insurance coverage cannot be bound or changed via submission of any online form/application provided on this site or otherwise, e-mail, voice mail or facsimile. No binder, insurance policy, change, addition, and/or deletion to insurance coverage goes into effect unless and until confirmed directly by Arabia Insurance Company. Any proposal of insurance we may present to you will be based upon the information you provide to us via this online form/application and/or in other communications with us and Arabia Insurance Company shall not be bound to cover you in case of fraud, false or incomplete declaration of information.

Products & services listed on E-Arabia may not have been registered or authorized by the central bank, governmental or regulatory authority in one or more of Arabia’s countries of operations or in the country of your residence. Accordingly, you may not have the benefit of protection of the laws and regulations of your country of residence with respect to products or services referred to on or sold through E-Arabia.

VI. Limited Liability

In no event will Arabia Insurance Company, its agents or employees, be liable for any damages, losses or other expenses arising in connection with E-Arabia or use thereof or inability to use by any party, or in connection with any fraudulent acts or failure of performance, error, omission, interruption, defect, delay in operation or transmission,

computer virus or line or system failure, even if Arabia Insurance Company, or its representatives, are advised of the possibility of such damages, losses or other expenses.

VII. Sanction Clause

Arabia Insurance Company will **not** accept/make any payment, perform a transaction, or provide any service or product if said payment, transaction, service or product would expose the Company to any sanction, fine, prohibition or restrictions under UN resolutions, trade or economic sanctions, laws or regulations applicable in the European Union, UK, USA, or other countries that affect the Company's business, or the laws or regulations in the countries in which the Company is active.

VIII. Consent

By transmitting information through E-Arabia, you consent to its use. You agree to be bound by any statement, affirmation, consent, or agreement you make or transmit through E-Arabia, including but not limited to any consent you give to receive records or communications from Arabia Insurance Company solely through electronic transmission.

You agree that we are under no obligation to confirm the identity or authority of any user of this Website. You accept the risk that the information you transmit to us and any information that we transmit to you may be intercepted by third parties.

IX. Questions

For additional information, please contact your nearest regional office:

<https://www.arabiainsurance.com/en>

Arabia Insurance Company.

Arabia Insurance Company (AIC)

Data Protection & Confidentiality Charter

The present document was first issued in August 2023 with the methodology and proposed structure. Any material changes that have subsequently been made to this framework are annotated with the calendar date in which the changes were made.

Abbreviations

AIC	Arabia Insurance Company
BOD/Board	Board of Directors
BT	Business Technology
CBB	Central Bank of Bahrain
CEO	Chief Executive Officer
Company	AIC Lebanon and its local and foreign branches
CISO	Chief Information Security Officer
DHA	Dubai Health Authority
DPO	Data Protection Officer
ERM	Enterprise Risk Management
GDPR	General Data Protection Regulation
HIA	Health Information Assets
HIPAA	The Health Insurance Portability
HIE	Health Information Exchange
ICT	Information and Communication Technology
IG	Information Governance
IP	Internet Protocol
ISMSC	Information Security Management System Committee
IT	Information Technology
KPIs	Key Performance Indicators
NESA	National Electronic Security Authority
PHI	Protected Health Information
RCC	Risk & Compliance Committee
SEM	Senior Executive Management
SSL	Secure Sockets Layer
UAE	United Arab Emirates
URL	Uniform Resource Locator
QCB	Qatar Central Bank

Table of Contents

I.	Introduction.....	11
II.	Scope of Application.....	11
III.	Regulatory Framework.....	11
IV.	Governance.....	12
IV.1.	CEO	12
IV.2.	The Information Security Management System Committee	13
IV.3.	The Chief Information Security Officer	13
IV.4.	Data Protection Officer	13
IV.5.	Information Governance (IG) Manager.....	14
IV.6.	Line Managers.....	14
IV.7.	All Staff.....	14
IV.8.	Risk Management	15
V.	Data Protection and Confidentiality Principles.....	15
VI.	Protected Health Information.....	18
VI.1.	Processing.....	18
VI.2.	Data Subject Consent	18
VI.3.	Third Parties	19
VI.4.	Transfer & Disposal.....	20
VI.5.	Breach of Data Protection and Confidentiality	21
VI.6.	Incident Response & Reporting.....	21
VI.7.	Data Protection by Design and by Default.....	23
VI.8.	Data Subject Rights on Protected Health Information	23
VI.9.	Information Technology (IT) Systems.....	23
VI.10.	Hardware (Biomedical & non-biomedical) Management	23
VI.11.	Removable Media Management.....	24
VI.12.	PHI/HIA Physical Security and Access Control	24
VI.13.	Processing Protected Health Information through Nabidh Health Information Exchange (HIE)	24
VII.	Health Information Assets (HIA) Classification	25
VIII.	Health Information Assets Re-classification	25
IX.	Health Information Asset Labelling.....	26
X.	Health Information Assets Access Permissions within Arabia.....	26
XI.	Health Information Asset Management	26
XII.	Use of cloud-based solutions for Health Information Asset management	26
XIII.	Digitizing Medical Record.....	27

XIV. Business Continuity /Disaster Recovery Plans	28
XV. Training	28
XVI. Closing or Merging of Arabia	28
XVII. Accountability	28
XVIII. Monitoring and Compliance.....	29
XIX. Non-Compliance.....	29
XX. Annex – A.....	30
XXI. Annex – B.....	31
XXII. Annex – C.....	33
XXIII. Annex – D.....	34
XXIV. Annex – E.....	34

I. Introduction

In recent years, data privacy has become a much bigger concern for all companies, and especially more critical for companies serving in the health sector. Healthcare providers must ensure that they properly manage patient data to create a culture of trust and transparency with patients while meeting strict data privacy and legal regulations. Data privacy in healthcare is constantly evolving with continuously updated laws and regulations.

As an insurance company for over 75 years with a presence in 8 Arab countries, Arabia Insurance Company (Arabia or AIC) naturally provides medical insurance coverage for its clients and therefore deals with sensitive personal information. Because Protected Health Information (PHI) is among an individual's most sensitive (and for criminals, valuable) private data, the guidelines for healthcare providers and other organizations that handle, use, or transmit patient information include strict data protection requirements that come with hefty penalties and fines if not met.

II. Scope of Application

The guidelines and procedures included in this Charter are applicable to AIC Lebanon and all local and foreign branches in Arabia's areas of operations including all systems, employees, and other third parties who have access to its systems. In order to comply with the best practices standards, the present Charter takes into consideration all the guidelines and rules required by the different regulators of AIC's foreign branches including AIC Bahrain, AIC Kuwait, AIC Qatar, and AIC UAE. Therefore, circulars and regulations regarding Health Data Protection and Confidentiality issued by the regulators in those countries were incorporated as well in the present Charter.

III. Regulatory Framework

The present Charter is based on laws and regulatory requirements issued by the United Arab Emirates (UAE) and the Emirate of Dubai legislative/regulatory frameworks. These include:

- UAE Federal Law No. (2) of 2019 concerning the use of the Information and Communication (ICT) in the area of Health ("ICT Health Law") and its exemptions.
- Resolution No. (2) Of 2017 Approving the Policies Document on Classification, Dissemination, Exchange, and Protection of Data in the Emirate of Dubai.
- Telecommunications and Digital Government Regulatory Authority (TDRA) of the UAE rules and regulations.
- Executive Decision (51) of 2021 entitled "UAE ICT Health Law".
- UAE Federal Data Protection Law No. (45) of 2021 entitled "UAE Data Protection Law".
- Federal Ministerial Decision No. 51 of 2021 Cases Allowing the Storage and Transfer of Medical Data and Information Out of the UAE.
- The Dubai Health Authority (DHA) "Health Information Assets Classification Policy."
- The National Electronic Security Authority (NESA).
- The EU's General Data Protection Regulation (GDPR).

- Dubai Government Information Security Regulation (ISR) rules and regulations.
- Information Security Management System (ISMS), ISO 27001.
- Cabinet resolution No. (40) Of 2019 and Federal Decree-Law No. (4) Of 2016, Concerning the Executive Regulation of on Medical Liability and Addendum Regulations and Conditions for Providing Telehealth Services.
- UAE federal, and Emirate of Dubai Electronic Security Authority standards and guidelines for cyber security.
- DHA IG policies (e.g. Nabidh policies and standards, Health Data Protection & Confidentiality policy, Health Data Quality policy, and Health Data Security Policy).
- "Dubai Electronic Security Centre" requirements as applicable.
- "Smart Dubai Government" regulations and requirements as applicable.
- DHA-Dubai health insurance corporation requirements for e-claims, reimbursement, and documentation as applicable.

When it comes to health data, the DHA regulation for Health Data Protection and Confidentiality issued in August 2022, was designed to ensure that insurance entities falling under the jurisdiction of the DHA are providing a secure environment for data management, specifically Protected Health Information.

Arabia shall strive to uphold its responsibilities regarding personal data protection by adhering to the above applicable legal, statutory, and regulatory requirements. In addition to this, Arabia must adhere by the following.

- Section (4.21) of DHA *Policy for Health Data Protection and Confidentiality*, Version 1, 2022
- Section (4.18) of DHA *Policy for Health Information Assets Classification*, Version 1, 2021
- Section (4.19) of DHA *Policy for Policy for Health Information Assets Management*, Version 1, 2022

IV. Governance

The following section states the roles and responsibilities of the different parties in relation to the preparation and approval of the Data Protection and Confidentiality Charter.

IV.1.CEO

The Chief Executive Officer (CEO) has the ultimate responsibility for ensuring that suitable arrangements are in place for the management of Data Protection and Confidentiality, in the form of policies that support the implementation, use, and handling of data (including PHI). These policies should also ensure that the processing of data is done transparently, lawfully, accurately, securely and with a lawful basis in line with the Data Protection and Confidentiality Principles.

The CEO is also responsible for ensuring that sufficient resources are provided to support the requirements of the Charter and the role of Data Protection Officer including the necessary IT systems, staff, budget, etc.

IV.2.The Information Security Management System Committee

The Information Security Management System Committee (ISMSC) represents the management commitments towards information security at Arabia. This includes the relevant policies and procedures including Data Protection and Confidentiality. Membership of this committee includes senior management members from business functions, IT, Risk and Compliance.

The responsibilities of the ISMSC with respect to Data Protection and Confidentiality include:

- Review and approve the Data Protection and Confidentiality Charter.
- Determine and provide resources to plan, implement, monitor, review and improve information security and management.
- Ensure that IT systems within the Company have adequate controls in place to prevent loss, unlawful processing, or inappropriate access to data.
- Check that arrangements that involve external organizations having access to information systems are based on a formal agreement that defines all necessary security requirements.
- Report to the RCC any outstanding issues such as status reports, staff information security awareness, updates on any cyber security incidents/breaches, results from internal/external assessments, etc.

IV.3.The Chief Information Security Officer

The ISMS function is headed by the Chief Information Security Officer (CISO) who has the following responsibilities with respect to Data Protection and Confidentiality:

- Report to the ISMS on all security related matters on a regular basis.
- Communicate information security policies to all relevant personnel and customers where appropriate.
- Quantify and monitor the types, volumes and impacts of security incidents and malfunctions.
- Ensure that procedures are in place to define the recording, prioritization, business impact, classification, updating, escalation, resolution, and formal closure of all security incidents.
- Provide appropriate training and awareness program to all staff at least every 2 years to support compliance with the Data Protection and Confidentiality Charter and all the relevant regulation.

IV.4.Data Protection Officer

The UAE Data Protection Law requires all Entities and data Processors to nominate/appoint Data Protection Officer (DPO), who has the requisite professional qualities and expert knowledge of data protection compliance.

The DPO can be an employee within the Company or an external appointed party. Arabia shall assign responsibility of data controller to its Compliance Manager. Arabia will share the contact details of the appointed DPO with UAE Information Office and DHA.

The roles and responsibilities of the DPO include:

- Overseeing implementation of data protection and security measures to ensure compliance with all related regulations.
- Ensure the legitimacy and accuracy of the data protection process.
- Receiving and handling all complaints on data protection and confidentiality
- Providing technical advice regarding data protection assessments, periodic PHI inspection procedures, and anti-breach systems under use.
- Documenting all data protection assessments and risk management procedures.
- Reporting directly to the CEO and the Board of Directors.
- Advising colleagues, employees, contractors, consultants, suppliers, vendors, and partners on data protection compliance.
- Conducting awareness on the applicable laws and regulations related to Data Protection and Confidentiality, including the development of policies, procedures, and guidance to the all the relevant parties within the Company.
- Acting as the Company's main point of contact with the Regulators including the UAE Information Office and DHA.
- Maintaining confidentiality of data, especially PHI.

IV.5.Information Governance (IG) Manager

The Information Governance (IG) Manager (or the job title assigned with responsibilities of managing IG) is responsible for enforcement and endorsement of this Charter.

The IG Office/Section (or the function assigned with IG responsibilities) is responsible to support the relevant business Office/Section in implementation of the defined controls and ensuring compliance with this Charter. The IG Office/Section (or the function assigned with IG responsibilities) is responsible to conduct awareness about the Charter to Users. Any compromise of HIA/PHI must be reported to IG office/section.

IV.6.Line Managers

Line Managers are responsible for maintaining data protection compliance within their departments and ensuring that their permanent or temporary staff and contractors are aware of:

- The Data Protection and Confidentiality Charter as it relates to their work areas.
- Their personal responsibilities for handling PHI.
- Compliance with reporting requirements.
- How and where to access advice on handling PHI.
- Ensuring their staff have undertaken the Entity's mandatory training.

IV.7.All Staff

All staff employed by Arabia are affected by the UAE Data Protection law:

- They have rights as employees about whom Arabia is holding data.
- They have obligations as healthcare professionals who collect data about Data Subjects.

All staff must:

- Understand their legal obligation to keep PHI confidential, to ensure they do not breach the data protection principles and uphold the data subject's rights.
- Participate in induction, mandatory and awareness training sessions.

- Be aware of the nominated Data Protection leads in the Entity.
- Challenge and verify where necessary the identity of any person who is making a request for confidential information and determine the validity of the reason for the request.
- Report actual or suspected breaches of confidentiality to their line manager.

All Employees who handle Confidential, Sensitive, or Secret data assets:

- Must sign an Employee Confidentiality Agreement / Non-disclosure Agreement.
- Must understand the impact of these legal frameworks, and how it relates to their role.
- Should be supported by training as appropriate.

IV.8.Risk Management

Risk Management is a control function and has the responsibility to establish a comprehensive risk management process, which ensures the timely identification, measurement, monitoring and reporting of risks including those that might compromise data.

The main responsibilities of risk management include:

- Assist the CISO in the development of the Data Protection and Confidentiality Charter in line with regulatory requirements and best practices.
- Ensure AIC compliance with the controls and procedures of the Charter.
- Report to management on any changes or updates to the Charter.
- Develop and review the Information Security policies and procedures under the scope of the AIC Enterprise Risk Management (ERM) Framework.
- Coordinate with different departments/functions (including Business Technology (BT), Compliance, Legal, etc.) on the review and update of the Information Security Risk Management Framework including different policies related to Cyber Security, Data Protection and Confidentiality, etc.
- Risk assessment of potential impact of disclosure based on Annexure – A.

V. Data Protection and Confidentiality Principles

Arabia considers its responsibility to protect and secure all types of personal information (including health information) that it collects from its customers, employees, etc. The following principles describe the basic requirements regarding the handling of such information:

Fairness, Lawfulness and Transparency

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means. Data subjects have the right to consent to granting data before it is processed.

The processing of PHI must be lawful, fair, and in a transparent manner.

Purpose Limitation

The purposes for which personal data are collected should be specified no later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes and as are specified on each occasion of change of purpose.

PHI must be collected for specified, clear, and legitimate primary use purposes and not further processed in a manner that is incompatible with those purposes. Any PHI given or received in confidence for one purpose may not be used for a different purpose or passed on to anyone else without the consent of the Data Subject

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Purpose Specification mentioned above, except:

- With the consent of the data subject; or
- By the authority of law.

Any secondary use (ex: research, quality improvement, defending a legal claim or Complaint, etc.) of PHI should require adherence to the UAE ICT Health Law:

- Arabia must justify the purpose(s) for using PHI for secondary use.
- The purpose of the secondary use of PHI must be recorded by the Entity.
- Secondary use (e.g. Research, Public Health, Clinical Audit and Quality Improvement, Safety Initiatives, Facility Accreditation Purposes, Prosecuting or Defending a Legal Claim or Complaint, and marketing). of PHI should require further permission/approval from DHA (HISH@dha.gov.ae).

Data Minimization

PHI must be adequate, relevant, and not excessive, and should remain limited to what is necessary in relation to the purposes for which they are processed.

Protected health Information must be kept in a form that permits identification of Data Subjects for no longer than is necessary for the purposes for which the data is processed.

Accuracy

Arabia shall measure data quality based on accuracy while taking reasonable steps to ensure PHI is accurate, complete, and up to date. Arabia should ensure every sensible step is taken to ensure that inaccurate PHI are rectified immediately.

Security Safeguards

Personal data should be protected by reasonable security safeguards against risks such as information leakage/loss or unauthorized access, destruction, use, modification, or disclosure of data.

Arabia must guarantee the integrity and confidentiality of PHI at all circumstances.

Physical & Environmental Security

The physical environment and its security measures must be diligently maintained to facilitate the secure processing, storage, communication/sharing, hosting, and disposal of Health Information Assets (HIA). Various measures and controls must be considered by the Entity to safeguard HIA from potential connectivity loss, ensuring uninterrupted availability of information processing and storage equipment, and protecting medical

devices from a range of threats including theft, fire, flood, intentional or unintentional damage, mechanical failure, and power failure. Adequate physical security measures should be implemented to address foreseeable threats, subject to periodic testing for effectiveness.

Arabia should take into account several aspects of physical and environmental security, encompassing the protection of data centers and information processing facilities, control of physical entry to secure areas, safeguarding medical devices, ensuring appropriate heating, ventilation, and air conditioning, maintaining supporting mechanical and electrical equipment, conducting surveillance of critical areas, securing physical archives, implementing fire and environmental protection measures, and managing visitor access.

Retention/Storage/Archival/Reuse

Arabia's Policy for Retention, Storage, Archival, and Reuse of Health Information Assets (HIA) mandates the secure retention and storage of HIA based on their classifications within UAE-based data centers.

Compliance with UAE laws and regulations, including obtaining approval from DHA_HISHD and adhering to UAE ICT law exemptions, is paramount. The information asset owner is tasked with ensuring adherence to specified retention periods, with a minimum retention period of 25 years for health data as per UAE ICT Health Law. Arabia must establish and enforce archival criteria and methods, ensuring data preservation and meticulous record-keeping. Appropriate security controls must be applied throughout the storage, archival, and reuse processes to prevent unauthorized access or disclosure. While HIA may be reused for legitimate purposes, data must not be retained beyond necessary durations, and Arabia must securely dispose of data, including pertinent Personal Health Information (PHI), when retention grounds cease. Reference to the UAE ICT Health Law and DHA policies is essential for compliance with health information retention timelines. Suggested HIA storage requirements are mentioned in Annexure – D.

Retention of HIAs to be followed by the requirements mentioned in the policy document “Policy for Health Information Assets Management, Version 1, 2022”, section 4.6, 4.7, 4.8, 4.9, 4.10.

Storage of HIAs to be followed by the requirements mentioned in the policy document “Policy for Health Information Assets Management, Version 1, 2022”, section 4.11.

Individual Participation:

Every individual data subject should have the right to:

- To obtain from Arabia, or otherwise, confirmation of whether the Company has data related to the data subject, as well as the purpose of processing it and the source and recipient entities that will process the data.
- To have communicated to him/her, data relating to him/her:
 - o within a reasonable time.
 - o at a charge, if any, that is not excessive.
 - o in a reasonable manner.
 - o in a form that is readily intelligible to him.

- To be given reasons if the data request is denied, and to be able to challenge such denial.
- To challenge the data given and, if the challenge is successful to have the data erased, rectified, completed, or amended.

VI. Protected Health Information

The below sections describe the manner with which Arabia will process and manage PHI.

VI.1. Processing

PHI is detailed personal information of the data subject that includes any of the 18 types of identifiers specified below:

1. Name (Full name as per passport or Emirates ID).
2. Address (All geographical identifiers).
3. All elements of dates (other than years) related to an individual (including birth date, admission date, discharge date, date of death and exact age if over 89).
4. Telephone numbers.
5. FAX number.
6. E-mail address.
7. Identification Number based on country of residence (ex: Emirates Identification Number).
8. Medical record number.
9. Health insurance beneficiary numbers.
10. Bank Account number.
11. Driving license number.
12. Vehicle identifiers (including serial numbers and license plate numbers).
13. Device identifiers or serial numbers.
14. Web Uniform Resource Locators (URLs).
15. Internet Protocol (IP) address numbers.
16. Biometric identifiers, including finger, retinal and voice prints.
17. Full face photographic images and any comparable images.
18. Any other unique identifying number, characteristic, or code.

Processing of PHI within the Entity must be lawful and safe and as per the applicable laws and regulations in Arabia's counties of operation including the UAE federal laws, Emirate of Dubai legislations, and DHA regulations. The Company should maintain routine data processing within the framework of confidentiality and privacy.

VI.2. Data Subject Consent

The Company must inform Data Subjects and service users about how their PHI is used and to whom it may be disclosed.

Secondary use (e.g., Research, Public Health, Clinical Audit and Quality Improvement, Safety Initiatives, Facility Accreditation Purposes, Prosecuting or Defending a Legal Claim or Complaint, and marketing) of identifiable health data needs consent from Subject Data.

As per UAE ICT Health law, anyone dealing with PHI must ensure its confidentiality. If PHI is used for secondary use purposes, then written consent of the Data Subject is required.

However, the Entity is legitimate to process the PHI without Data Subject consent, as per article (16) of UAE ICT Health law and article (4) of UAE Data Protection Law, in following settings:

- Protected health information is required by the health insurance companies or other health service providers for purposes of auditing, approving, or verifying the financial benefits related to services.
- For the purposes of scientific and clinical research, provided that the Data Subject's identity is not disclosed and that the ethics and rules of scientific research are followed.
- For protecting public health, such as protecting against communicable diseases / epidemics and serious cross-border threats to health; or to maintain the health and safety of the Data Subjects or any other persons in contact with them.
- At the request of the competent judicial authorities.
- At the request of DHA for the purposes of inspection, supervision, and protection of public health.
- For the Processing of PHI that are manifestly made public by the Data Subject.
- Processing is necessary for the investigation, establishment, exercise or defence of legal claims or potential legal claims including complaints to the Regulator against the Entity or its employees; or whenever courts are acting in their judicial capacity.
- For compliance with a legal obligation to which the Entity is subject.
- For the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.
- To ensure high standards of quality and safety of health care and of medicinal products or medical devices based on UAE laws and DHA regulations.
- For the purposes of conducting the obligations and exercising specific rights of the Entity (as Controller) or of the Data Subject in the field of employment, social security, and social protection law.
- For pursuant to a contract the Data Subject is part of it; or to take actions based on Data Subject request for pursuant/ modification/ or termination of a contract.

VI.3.Third Parties

Where processing is to be conducted on behalf of the Company by a third party or external vendor, Arabia should ensure that these entities are providing sufficient guarantees to implement appropriate technical and organizational measures in line with the

requirements of this Charter by issuing clear written authorisation clarifying the obligations and responsibilities of the data processor.

If Arabia instructs a third party, within the UAE, to process PHI on its behalf, a Data Sharing Agreement/Contract must be signed. The contract must include appropriate clauses setting out responsibilities for data protection and confidentiality, consistent with UAE Data Protection Law, ICT Health Law, and DHA policies (requirements. If no such clause exists within the data sharing agreement/contract, the supplier must complete and sign a separate Confidentiality Agreement.

The third party must abide with the health data protection and confidentiality terms even after the contract expires. In addition, any PHI transferred by the Entity outside the facility, but within the UAE, for processing, must be securely encrypted during transit.

Where PHI data/records need to be transported in any media, this process must be conducted to maintain strict security and confidentiality of this information. All portable electronic media must be encrypted.

When the PHI is transferred electronically, it should be abiding access control measures on privacy, security, and confidentiality (e.g., password-protected portals, encrypted Secure Sockets Layer (SSL), HIPAA compliant document transfer).

Protected Health Information should 'not be kept for longer than necessary' for which it is required for processing by third party.

Arabia has the responsibility on failure of a supplier or contractor to comply with this Charter. If any violations happened, Arabia must take the necessary legal action. The DHA_HISHD must be informed instantly (HISH@dha.gov.ae).

VI.4.Transfer & Disposal

Protected health information should not be transferred to a country or territory outside the UAE, except when this transfer is within the category of UAE ICT Health Law exemptions specified under the Health Data Protection and Confidentiality Policy issued by the DHA.

Any transfer or sharing of PHI to outside of UAE must be conducted securely (by encryption) and safely to prevent the risk of accidental disclosure or loss in transit.

As for the disposal of PHI, please refer to the UAE ICT Health Law and DHA policies which provide detailed guidance on the minimum retention periods applicable to HIA and disposal procedures.

It is worth noting that Arabia, has a legal obligation to maintain confidentiality standards for all HIA archiving and disposal. Moreover, the disposal of electronic equipment that may hold PHI such as PCs, laptops, and any other devices with information storage capabilities should be carried in a way ensuring all data is effectively removed before destruction.

Compliance with the retention requirements outlined in UAE federal, Emirate of Dubai, and DHA_HISHD laws, regulations, and policies is mandatory prior to the disposal of physical or digital data. All Health Information Assets (HIA) must undergo secure disposal in accordance with their classification at the end of their intended life cycle, with proper authorization from the HIA owner. The Entity must ensure that appropriate security controls are in place during the disposal process to render the information irrecoverable,

minimizing the risk of confidential information leakage. Formal procedures for secure disposal must be established to prevent unauthorized access to confidential information. Furthermore, the Entity is required to maintain a comprehensive log of all HIA reused or destroyed, treating all disposal media as confidential. Records of media disposal, including details such as the information asset owner, type of HIA, classification, disposal type, reason for disposal, retention expiry date (if applicable), data removal confirmation, evidence, and authorized personnel, should be maintained for audit purposes as per the retention policy. Destruction of media by a third party should be supervised, and the third party must issue a certificate of destruction. Suggested HIA disposal requirements are in Annexure – E.

Furthermore, destruction of HIA process will be followed as mentioned in the section (4.16) and record will be maintained in a register as mentioned in the section (4.17) of DHA policy “*Policy for Health Information Assets Management, Version 1, 2022*”.

VI.5. Breach of Data Protection and Confidentiality

A breach of security leads to the accidental or unlawful destruction, loss, alteration, concealment, unauthorized disclosure, or access to PHI transmitted, stored, or otherwise processed. Any breach or suspected breach of data protection and confidentiality can have severe implications for the health sector, Data Subjects, and employees.

Examples of offences which may be considered to be gross misconduct include:

- Unlawful disclosure of PHI.
- Inappropriate access to PHI, where there is no defined clinical reason.
- Inappropriate use/misuse of PHI.
- Loss of availability of PHI.
- Unauthorized disclosure or copying of PHI.
- Access to PHI by an unauthorized third party.
- Deliberate or accidental action (or inaction) by a Controller or Processor.
- Sending PHI to an incorrect recipient.
- Computing devices containing PHI being lost or stolen.
- Alteration of PHI without permission.
- Re-identification of de-identified PHI without the consent of the Data Subject.

Breaches of confidentiality or unauthorized disclosure of any information constitutes a serious disciplinary offence and gross misconduct.

VI.6. Incident Response & Reporting

Arabia has in place an Information Security Incident Response Procedure that covers several aspects under a set process that includes:

- Process to log, categorize, and prioritize an incident.
- Incident diagnosis.
- Incident escalation.
- Resolving and closing the incident.

The Incident Response Procedure also details corrective actions, investigation and collection of evidence processes, recovery of lost data and documentation procedures for lessons learned.

Breach investigations range from the point of discovery until full closure with collection of evidence such as screenshots, audit logs, manual records of incident chronology, original documents (if available) and details of any witnesses.

Once collected, the evidence should be kept at a safe place where it cannot be tampered with. The evidence may be required for:

- Later analysis to determine the cause of the incident.
- Forensic evidence for criminal or court proceedings.
- Support of any compensation negotiations with software or service suppliers.

The Entity is required to report breaches/incidents within the designated period defined by Executive Regulations of the relevant regulator. In the UAE, breach notifications must be reported to both the UAE Information Office and DHA (HISH@dha.gov.ae).

The report should include the following:

- Nature and type of breach.
- Date of breach.
- How the breach was discovered.
- Reasons of breach.
- Categories and approximate number of Data Subject concerned.
- Extent/severity of the breach and the potential consequences of it.
- Formal measures being taken by the Company and/or Data Processor for reporting, investigating, and recording breaches.
- Correcting procedures being taken by the Entity and/or data Processor.
- Information on data protection officer (DPO) within the Entity.

If the third party (data processor) identified any breach of data (especially PHI), it should be reported to Arabia immediately.

Where the PHI breach is likely to result in a high risk to the privacy and confidentiality of the Data Subject, the Company must communicate it to the Data Subject within the designated period set by regulator in Arabia area of operations (e.g., as per UAE Data Protection Law).

The breach notification to Data Subject should describe in clear and plain language:

- The nature of the PHI breach.
- Likely consequences of the PHI breach.
- How the breach affected Data Subject privacy and PHI confidentiality.
- Name and contact details of the Entity's Data Protection Officer.
- Measures taken/or proposed to be taken to address the breach.

The Data Protection Officer in the Entity is the single point of contact for all breaches. Advice and guidance must be sought as soon as possible by contacting DHA HISH@dha.gov.ae.

VI.7.Data Protection by Design and by Default

Data protection should be seamlessly integrated from the outset of any new project, service, contract, or process. This entails incorporating data protection principles into all phases of PHI processing activities, including the implementation of safeguards such as data minimization, pseudonymization, and purpose limitation as prescribed in this Charter, thereby safeguarding individual rights throughout the data processing lifecycle.

VI.8.Data Subject Rights on Protected Health Information

Arabia is committed to respecting the rights of data subjects throughout the processing of their Personal Health Information (PHI) and will diligently adhere to all relevant laws and regulations, with particular emphasis on the UAE Federal Data Protection Law No. (45) of 2021, as well as the requirements outlined in Section 4.6 of the Policy for Health Data Protection and Confidentiality (Version 1, 2022) issued by DHA.

VI.9.Information Technology (IT) Systems

Arabia will ensure that IT systems within the company have adequate controls in place to prevent loss, unlawful processing, or inappropriate access. The detailed coverage of minimum access control standards concerning health IT systems will be included in the company's information security policy.

VI.10. Hardware (Biomedical & non-biomedical) Management

- Hardware must be controlled and accounted at all times through the Asset management Department or (if biomedical equipment) Clinical Engineering Department.
- All hardware must be assigned an owner specified in the Asset register.
- There must be a record of the movements of all hardware containing PHI, containing the owner and the designated individual(s) responsible for the movement.
- The movement of hardware must be authorized and logged by the appointed HIA management department within the Arabia prior to the hardware and electronic media entering or leaving a facility.
- The HIA management department within the Arabia must be accountable for hardware while in transit between facilities.
- Hardware must be properly logged and securely disposed of when no longer used.
- Protected Health Information must be removed from hardware before it is made available for reuse or dispose; and there shall be a reasonable assurance that the disposed data is not recoverable.
- A retrievable, exact copy of PHI, (when needed or requested) must be created before any movement of hardware.
- Before destructing HIA media, it must be sanitized by reformatting the hard drive in a secure manner or by using a wipe out utility.

VI.11. Removable Media Management

- Removable media must be stored in secure environment and in accordance with the manufacturer`s specifications. Previous contents of any re-usable media must be completely erased before handing it to next custodian and reasonable assurance must be provided that the data is not recoverable.
- Wherever mandated, cryptographic techniques must be applied to protect data on removable media.
- Health information assets sent outside the Entity for repair or data recovery must be protected from disclosure by mutually agreed contract.
- Record of the HIA movement must be maintained to keep an audit trail.

VI.12. PHI/HIA Physical Security and Access Control

Arabia must develop and implement policies and procedures that restrict access and usages of PHI/HIA based on the specific roles of their staff, trainees, vendors and third-party contractors.

- The policies and procedures must identify:
 - o The persons, or classes of persons, within the Entity who need access to PHI to carry out their duties.
 - o The categories of PHI to which access is needed.
 - o Any conditions under which they requisite the PHI to do their jobs.
- Users must only access PHI for those Data Subjects that they have authorisation to access for specific purposes.
- Any access to records, which is not legitimate / authorised, is prohibited and unlawful.4.8.5. Staff have no right to access PHI held in records about their relatives/friends/ or co-workers, where they do not form part of the care team.
- Staff should not attempt to access or use electronic record systems they have not been trained to use or authorised to access.
- Existing system users should not allow others to access systems using their login credentials. Sharing system passwords is a disciplinary offence and viewed as a serious breach.
- The Entity must carry out audits of access to PHI; and any member of staff who is found to be in breach of this guidance by inappropriately accessing PHI must face disciplinary action.
- The unauthorised access to the Entity`s computer systems including hacking and the subsequent use of that PHI is considered a criminal action.

VI.13. Processing Protected Health Information through Nabidh Health Information Exchange (HIE)

In compliance with data protection standards, the Entity must obtain consent from the Data Subject before accessing their PHI through Nabidh HIE. This consent should be straightforward and easily understood, whether provided in paper or electronic form. Additionally, the consent form should include an option for the Data Subject to opt out, with a simple and accessible process for doing so. Once given, consent remains valid until the Data Subject decides to opt out from HIE.

Data Subjects have the right to opt out of Nabidh HIE at any time, though this decision does not affect data processed prior to opting out.

VII. Health Information Assets (HIA) Classification

Information assets includes information/data in all its form, as well as the underlying application, technology, and physical infrastructure to support its processing, storing, communicating, and sharing.

The following are considered HIA:

- Information (in physical and digital forms)
- Medical device and equipment
- Applications and Software
- Information System
- Physical Infrastructure (Datacentres, access barriers, electrical facilities, HVAC systems, etc.)
- Human resources (in support of care delivery)

All HIA generated, processed, and stored by Arabia must be subject to classification into one of the following sets based on value and sensitivity of the information, and the consequences of information compromise:

- Open Data / Public
- Confidential
- Sensitive
- Secret

Information compromise includes, but is not limited to:

- Data loss
- Data misuse
- Data interference
- Data unauthorized access
- Data unauthorized modification
- Data unauthorized disclosure

The classification of HIA is wholly based on the examination of the value of the information, who will have access to the HIA, and the resulted risk impact if the information was compromised or accessed by unauthorized individuals. Refer to Annexure – B for the HIA classification.

VIII. Health Information Assets Re-classification

Arabia will assess the classification of the Health Information Assets (HIA) whenever necessary to reassess the potential impacts of any compromise. Reclassification of HIA may result in either an increase or decrease in its security classification. Declassification, on the other hand, involves the administrative decision to lower the security classification of HIA when it no longer requires heightened security handling. The responsibility for reclassifying HIA, whether to upgrade or downgrade its classification, lies with the information asset owner. Since reclassification entails changes in access control, appropriate precautions and security controls must be implemented to prevent information disclosure.

IX. Health Information Asset Labelling

All HIA regardless of its form (Electronic or physical) must be appropriately labelled based upon the security classification category identified and the level of confidentiality the information needs. To achieve clearly identifiable protective markings for physical documents, it is recommended:

- Using capitals, bold text, large font, and a distinctive colour (red preferred), for example SENSITIVE.
- Placing markings at the centre top and bottom of each page.
- Separating markings by a double forward slash to help clearly differentiate each marking.
- The labelling system needs to be clear and easy to manage.

X. Health Information Assets Access Permissions within Arabia

No individual is permitted to access Confidential/Sensitive/Secret Health Information Assets (HIA) without prior authorization from Arabia. The company must adhere to the principles of 'need to know' and 'minimum necessary' when granting access to Sensitive and Secret HIA, ensuring access is granted only to the extent required for the company's operations. Additionally, Arabia must conduct regular reviews to assess the ongoing necessity of HIA access. Furthermore, the company is responsible for implementing rules to safeguard data based on its classification, which may include access restrictions or encryption measures. For HIA access control requirements, refer to Annexure – C.

XI. Health Information Asset Management

- Health Information Asset (HIA) Management should be recognized as a specific corporate responsibility within Arabia.
- All HIA assets should be labelled, processed, and stored strictly in accordance with the classification levels assigned to them.

XII. Use of cloud-based solutions for Health Information Asset management

Before any cloud-based solution is implemented there are a number of measures to be considered:

- UAE laws and DHA regulations must be adhered to in selecting any cloud-based solutions for HIA management by the Entity.
- The cloud-based solution must provide adequate evidence that they follow UAE laws and legislations.
- The cloud-based solution must prevent handling and storing health information with a Cloud Service Provider (CSP), outside the legal jurisdiction or geographical boundaries of the UAE, including for CSP's Backup or Disaster Recovery purposes.
- Records in cloud storage must be managed as records in any other environment. The contractual contract for cloud storage must include a clause that:
 - o The continuity of cloud storage for the duration of contract is adhered to.

- In case of transfer of cloud storage to another vendor, the data should be returned to the Entity in a transferable format to retain the retention period.
- The CSP has no ownership rights on the stored data regardless of the format or storage medium.
- The CSP must have appropriate controls in place to dispose/destroy the health information if no longer required and provide reasonable assurance that data is not recoverable.
- Necessary measures must be taken to avoid any breach of protected health information stored in the cloud as per all UAE laws and DHA Data and Health Information Protection and Confidentiality Policy (Health Information Protection and Confidentiality Policy).
- Entities must make sure the health information stored in cloud-based solutions are available based on Subject Access process. If information was not found or was left unfound, it would be a breach of the Data Subject`s rights.

XIII. Digitizing Medical Record

- To improve the efficiency and management of Data Subject information, Arabia must digitize physical medical records into electronic format records (e-health records) after maximum Two (2) years of the release of this Charter.
- Assets that must be digitized include medical records, color text and documents.
- Assets that are preferred to be digitized include: laboratory assets and radiology images.
- Digital preservation must ensure that digital information remains accessible and usable.
- Quality control of digitized records must be conducted:
 - Digitized document images must be inspected visually / Scroll through to ensure scanned documents are complete, clear, and easily read.
 - Digitized records must be compared to the original paper document/physical record to ensure accuracy.
 - Digitized records must be accessible and readable for their full retention period. This includes finding the file, opening the file, and reading the file regardless of the software used in its creation.
- The content of physical records should only be destroyed once they have been digitized to the required standard and quality assurance of the digitized images has been completed, confirming that they are a like for like copy of the original physical records. The physical record itself can be destroyed after Sixty (60) days of quality control.
- If the condition of the original record prevents a good quality digitized image from being produced, the Entity should document the problem on the digitized record and indicate that the physical copy has been maintained and where it is located.
- Digital information must be recovered in an accessible format; in addition to providing information about those who have accessed the record.
- Digital continuity must be maintained in a way that digital information will continue to be available as needed despite advances in digital technology and the advent of newer digital platforms.
- Arabia must ensure that digitized records are stored in a secure folder and only available to those who need access to the records.

- Arabia must ensure the archived digitized records have required security controls.
- An inventory must be created providing information about who has accessed the digitized record and when.
- All incidents of potential data protection and confidentiality should be reported immediately to the Arabia's data protection officer.

XIV. Business Continuity /Disaster Recovery Plans

Arabia will insure that:

- It has documented business continuity policy and plan, disaster recovery plans in place for all its information assets, which can be activated in a timely manner to retain/retrieve HIA in case of service discontinuation in the event of disaster (natural, environmental, and human factors).
- These plans are tested regularly in order to maintain the integrity and availability of the information held.
- It will identify the competent trained staff responsible for business continuity and disaster recovery.

XV. Training

- Arabia must maintain appropriate training and awareness strategies to support compliance with this Charter.
- Data Security and Protection training is mandatory and must be provided to staff on induction and every 2 years to ensure they are aware of their confidentiality obligations in line with this Charter.
- Arabia must train all workforce members i.e. employees, trainees, vendors, contractors, and anyone over whom the Entities exercise direct control on its privacy policies and procedures, as necessary and appropriate for them to carry out their functions.
- Arabia should have a process to periodically review the competency of the staff and other resources including third party vendors.
- Arabia should review the training and awareness courses periodically to reflect current and updated applicable laws and regulations, including (UAE laws and DHA health data governance regulatory requirements).

XVI. Closing or merging of Arabia

- The obligation to make HIA available to Data subjects/patients and other healthcare professional continues even after closure/merger of Arabia as defined in the section (4.18) of DHA policy "*Policy for Health Information Assets Management, version 1, 2022*".

XVII. Accountability

- Arabia is responsible for complying with all applicable laws and regulations, including (UAE laws and DHA's policies and regulations), and must demonstrate its compliance.
- Arabia has a legal obligation to maintain confidentiality standards for all PHI.

- Arabia must undergo periodic internal and external audits and independent reviews to monitor compliance with the data protection requirements as specified in this Charter.
- Arabia must retain and provide the outcomes of the audit / compliance to DHA on yearly basis (hish@dha.gov.ae).

XVIII. Monitoring and Compliance

Entities must adhere to this Charter. The Entity is required to establish a plan for monitoring compliance, ensuring ongoing assessment of overall adherence to this Charter. Appropriate controls, encompassing physical, procedural, and technical measures, should be implemented in alignment with the sensitivity of the information. The IG Office/Section (or designated entity with IG responsibilities) is responsible for periodically verifying compliance with this Charter.

Any deviations from this Charter, supported by valid business justifications, necessitate approval from DHA_HISHD as the certified authority in accordance with ICT law. Entities are anticipated to furnish a Declaration of Maturity obtained from a competent third-party regarding information classification and handling, to be integrated into their Annual Report. This process should be facilitated or overseen by the IG Manager (or individuals holding positions responsible for managing the Entity's business divisions and sections).

In instances where certain IG technical roles are unavailable within the Entity, outsourcing to a competent consultancy company is advised. Users who encounter uncertainties or lack clarity regarding any aspect of this Charter should seek clarification or guidance from DHA_HISHD (HISH@dha.gov.ae).

XIX. Non-Compliance

A failure to adhere to this Charter is considered a violation that requires investigation; and disciplinary action / dismissal will be taken in accordance with the provision of the current legislations.

XX. Annex – A

Security Objective	Potential Impact		
	Low	Moderate	High
<p>Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy & proprietary information</p>	<p>The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</p>
<p>Integrity Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.</p>	<p>The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</p>
<p>Availability Ensuring timely and reliable access to and use of information.</p>	<p>The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</p>

XXI. Annex – B

Classification	Category Description	Risk Impact of Information Compromise	Examples
Open Data / Public	<ul style="list-style-type: none"> - Information intended to be used in public domain or public use, and has no legal, regulatory, or organizational restrictions for its access and/or usage. - Intended purpose from the creation, access and use of the information is the general advancement of society, promotion of the interest of the organization and of the country, providing essential information equipping citizens, patients and other stakeholders understand better the country's/ governmental/organizational vision and values. - Encryption recommended. - The use and release of open data must comply with applicable copyright laws. 	No Impact	<ul style="list-style-type: none"> - Public Domains - Patient information leaflets. - Press release / announcements. - Regulatory filings, such as Internal Revenue Service filings - Certification labels such as The Joint Commission Certification - Research publications. - General public health awareness or regulation awareness publications - General sales or marketing materials - Business contact information. - Etc.
Confidential	<ul style="list-style-type: none"> - Information that must be afforded limited confidentiality protection due to its use in the day-to-day operations. - Information that relates to the internal functioning of the Entity and will not have general relevance and applicability to a wider audience. - Although individual items of information are not sensitive, taken in aggregate they may reveal more information than is necessary if they were to be revealed. 	<ul style="list-style-type: none"> - Its compromise may violate UAE federal law, Emirates of Dubai local law, and/or DHA policies and regulations. - Cause limited damage to the public interest, Entity/ individual reputation, - Limited financial aspects damage. - Adversely affecting the Entity by limiting its competitiveness - Adversely affecting public safety or justice. 	<ul style="list-style-type: none"> - Routine business operations and services. - Minutes of meetings, internal Policies, Standard - Operating Procedures and Internal Circulars, Contract of non-critical projects, projects charters, and Entity's performance reports. - Correspondence within the Entity or with other Entities or third parties. - Financial reports and transactions. - Confidential decision-making documents. - Internal regulations, policies, standards, procedures. - Etc.

Classification	Category Description	Risk Impact of Information Compromise	Examples
Sensitive	<ul style="list-style-type: none"> - Information that requires strong protection due to its critical support to decision-making within the Entity, across health sector, and government. - Information that could disclose designs, configurations, or vulnerabilities exploitable by those with malicious intent. - Information that the Entity, or through government or regulatory mandates, has a duty of care to others to hold in safe custody. 	<ul style="list-style-type: none"> - The compromise of this information might violate UAE federal law, Emirates of Dubai local law, and/or DHA policies and regulations. - Lead to significant disruption/loss of emergency and health care capabilities, loss of public trust in the health sector, or significant loss of reputation to the health sector with momentous coverage by the national and international press. - Adversely affecting the Entity by limiting its competitiveness. - Adversely affecting public safety or justice. 	<ul style="list-style-type: none"> - Medical records and Personal health information. - Sensitive medical information: <ul style="list-style-type: none"> o Chemical dependency, o Human immunodeficiency virus infection o Mental health conditions o Behavioural health information o Psychotherapy notes, o Alcohol and substance abuse, o Reproductive health, o Genomic information, o Sexual health (including sexually transmitted diseases), o Child pregnancy data o Child abuse conditions. - Strategic/critical projects contract or RFPs - Audit reports. - Risk/assets registers. - Financial details in relation to projects or proposals - Information security incidents reports - Human resource files/Personal information about staff/Personally Identifiable Educational Records/Confidential information about the management of the Entity. - Court proceedings. - Adoption records. - Disciplinary records, complaints, investigations minutes, violations. - Agreements or contracts of a secret nature between the Entity and another Entity within the UAE or internationally. - Etc.

Classification	Category Description	Risk Impact of Information Compromise	Examples
Secret	Information that requires significant and multilevel protection due to its highly sensitive nature	<ul style="list-style-type: none"> - The disclosure of such information to the public or exchange within the Government on other than an authorized basis is illegal and may cause very serious damage to the Individuals, government, national security, social cohesion, economic viability, and health of the country. - Information compromise could potentially threaten life; seriously prejudice public order, triggering discrimination, mistreatment, humiliation or undermining people's dignity or safety. 	<ul style="list-style-type: none"> - Medical record of Very Important Person (VIP). - Security forces data. - Security reports, minutes, or orders. - Sensitive minutes and report of executive council and its committees. - Agreements/contracts between the Emirate of Dubai and another Emirate or between the UAE with another country. - Data relevant to witnesses of serious lawsuits. - Credit Card Details/Credit Card Details/Payment card information. - Controlled Technical Information ("CTI") - IP addresses. - Network & Infrastructure Diagrams. - Etc.

XXII. Annex – C

Health Information Assets Access Control Requirements			
Open Data / Public	Confidential	Sensitive	Secret
<ul style="list-style-type: none"> - Available to the public. - Can be shared with third parties with no permission. 	<ul style="list-style-type: none"> - Available to authorized users. - Shared by HIA owner consent. 	<ul style="list-style-type: none"> - Available only to authorized users. - Information asset owners must consider more Stringent access control. - Sharable across Government /Private Entities: <ul style="list-style-type: none"> o With the consent of the individual. o As required by contract, subject to appropriate non-disclosure restrictions and data sharing agreement. o Pursuant to a waiver of authorization issued by an authorized Institutional Review Board. - Access must be logged and reviewed by the information asset owner. 	<ul style="list-style-type: none"> - Access to this information may be distributed only: - If required by law or regulation. - Pursuant to a lawfully issued order. - If necessary, in the course of a legal proceeding.

XXIII. Annex – D

Health Information Assets Storage Requirements				
Category	Open Data / Public	Confidential	Sensitive	Secret
Printed Material	No special handling	<ul style="list-style-type: none"> - Store in a secure area. - Maintain a clear desk. Workforce members should “clear their desks” at the end of each workday. - Documentation must be labelled accordingly as Confidential/Sensitive/Secret. - Physical and environmental security measures (e.g. backups, storing in a fireproof cabinet, etc.) must be maintained to enable secure HIA processing, storage, communication/sharing, hosting, and disposal. 		
Electronic Documents	No special handling	<ul style="list-style-type: none"> - Storage on Entity`s-approved devices is required. - Control access and print capability. - Store on secure network drives only (not on hard drives or desktops). - Documentation owned and/or created by Entity must be labelled accordingly as Confidential/ Sensitive/ Secret. 		
Medical devices and equipment	-	Specific attention to access control, authentication, authorization, handling procedures, risk log and disposal of medical equipment and devices is required.		
Electronic media (memory sticks, hard drives, CDs)	No special handling	<ul style="list-style-type: none"> - Storage on Entity`s-approved devices is required. - Control access and print capability. - Store in a secure place. - Use Entity`s-approved encryption. 	<ul style="list-style-type: none"> - Backup media must be physically secured. - Backup media stored offsite must be encrypted. - Backup media must be made unreadable before 	
Mobile Devices	No special handling	<ul style="list-style-type: none"> - Mobile devices must be configured to prevent unauthorized use. - All mobile devices must employ encryption. - Connections between authorized mobile devices and EMRs must be encrypted. - Mobiles should be stored on secure place. 		
E-mail	No special handling	<ul style="list-style-type: none"> - Secret data must not be shared through email. - for Sensitive data: <ul style="list-style-type: none"> - Use of corporate email system is required. - Limit the amount of personal health information being sent to only what is necessary. - Ensure that no personal health information is in the subject line of the email. - Personal health information should be sent as: <ul style="list-style-type: none"> o A secure, locked (e.g. .pdf) attachment which requires a password to open. Or as a link to the health information portal. - Read/received/delivery receipts should be used where possible. - Add a disclaimer to your signature that indicates that the email is confidential and intended only for the intended recipient. It should also instruct anyone who receives an email in error to delete or shred the misdirected mail and notify the sender. - Copies of the email and attachments should be maintained in the client file. The date, time, addressee of the email should be apparent. 		

XXIV. Annex – E

Health Information Assets Resue / Destruction Requirements

Category	Open Data / Public	Confidential	Sensitive	Secret
Printed Material	No special handling. Consider recycling	Must be discarded in appropriately identified document container for shredding or destruction (except if subject to a legal hold).		
Electronic media (memory sticks, hard drives, CDs)	No special handling.	<ul style="list-style-type: none"> - Media subject to a legal hold may not be reused. If other media are to be reused, all data must first be removed by Information Services. - Disposal of electronic media should be in a secure manner. - All discarded media must be destroyed following the requirements of ISO 27001:2013 and Information Security Regulation (ISR) standards from Dubai Smart Government. 		