حكومة دبي
GOVERNMENT OF DUBAI

هيئة الصحة بدبي
DUBAI HEALTH AUTHORITY

نابض
NABIDH

Unifying Dubai's Healthcare

Policies and Standards

September 2020 (v1.0)

1. INTRODUCTION

The health system of the Emirate of Dubai comprehends the full spectrum of health services, and is accessible to all residents of the Emirate of Dubai. The Dubai Health Authority (DHA), is the regulative body of the health system in the Emirate of Dubai. The authority emphasizes on excellence in healthcare services by regulating and monitoring the health status of the community.

Health Regulation Sector (HRS) forms an integral part of DHA and is mandated by DHA Law No. (6) Of 2018, to shape the regulatory framework for the healthcare system, inspect against available regulations, enforce regulations, and encourage the adoption of Best Practices and performance targets by all health service providers. Health Regulation Sector explicitly undertakes the health regulation by developing policy, standards, and guidelines to improve healthcare quality and subject of care safety. It is also in charge of promoting the growth and development of the health sector in the Emirate of Dubai.

The manual for NABIDH (Health Information Exchange) Policies and Standards aims to fulfil the following overarching DHA Strategic Objectives and Program within the Dubai Health Strategy (2016–2021):

- Objective 1: Position Dubai as a global medical destination by introducing a value-based, comprehensive, integrated and high-quality service delivery system.
- Objective 2: Direct resources to ensure happy, healthy and safe environment for Dubai population.

- Strategic Program 10: Excellence and Quality, which promotes excellence in healthcare service delivery in Dubai while enhancing subject of care happiness, experience, satisfaction and trust.

2. ACKNOWLEDGMENT

The Health Regulation Sector (HRS) developed this Policy in collaboration with Subject Matter Experts. HRS would like to acknowledge and thank these professionals for their dedication toward improving quality and safety of healthcare services.

Health Regulation Sector

Dubai Health Authority

TABLE OF CONTENTS

Table of Tables

3. EXECUTIVE SUMMARY

The Health Informatics and Smart Health Department's (HISHD) mission is to improve access, quality, health status and efficiency in health sector in the Emirate of Dubai. One of the HISHD`s main objectives is to expand access to high-quality Health Information and facilitating the efficient flow and exchange of information among subject of cares, healthcare providers, funders and regulators with a focus on transparency and confidentiality and a balance between standardization and autonomy. This will be achieved by developing the necessary policies and standards for implementing and managing the Health Information systems in the Emirate of Dubai.

The NABIDH manual of policies and standards contributes to enhanced healthcare delivery, facilitating continuity of care, and better decision making while delivering cost savings. Health Information Exchange Interoperability is seen by the DHA as a state of readiness to deal with new technologies, clinical practices and changes in policies. Dubai Health Authority's aim is to provide a standardized electronic health system for describing the specific items and services provided in the delivery of health care in the Emirate of Dubai.

4. DEFINITIONS

Term	Definition
Access Control	A means of ensuring that the resources of a data processing system can be accessed only by authorized entities in authorized ways.
Affiliate	In relation to a Party, each other entity that directly or indirectly Controls, is directly or indirectly Controlled by or is under direct or indirect common Control with, that Party from time to time.
Anonymization	Process that removes the association between the identifying data set and the data subject.
Audit	Systematic and independent examination of accesses, additions, or alterations to electronic health records to determine whether the activities were conducted, and the data were collected, used, retained or disclosed according to organizational standard operating procedures, policies, good clinical practice, and applicable regulatory requirement(s).
Audit Log	An electronic record of chronological sequence for access to the NABIDH Platform, which includes queries made by Authorized Users, type of information accessed, information flows, and disclosed information along with date and time markers for those activities between the NABIDH Platform and Participants.
Audit Record	Record of a single specific event in the life cycle of an electronic health record.
Audit Record Repository (ARR)	Receives and stores audit records from sources and consumer of the NABIDH managed Health Information.
Audit Trail	Collection of Audit Records from one or more Audit Logs relating to a specific Subject of Care or a specific electronic health record.
Audit Trail and Node Authentication (ATNA)	IHE-ATNA Integration Profile establishes security measures which, together with the Security Policy and Procedures, provide patient information confidentiality, data integrity and user accountability. The Audit Trail and Node Authentication (ATNA) Integration Profile: contributes to access control by limiting network access between nodes and limiting access to

Term	Definition
	each node to authorized users. Network communications between secure nodes in a secure domain are restricted to only other secure nodes in that domain. Secure nodes limit access to authorized users as specified by the local authentication and access control policy.
Authentication	The process of reliable security identification of subjects by incorporating an identifier and its authenticator.
Authorization	The granting of rights, which includes the granting of access based on access rights.
Authorized User	An individual who has been authorized by a Participant or NABIDH to access Health Information via the NABIDH Platform in accordance with the Policies.
Availability	The property of being accessible and useable upon demand by an authorized entity.
Basic Patient Privacy Consents (BPPC)	IHE-BPPC provides a mechanism to record the patient privacy consent(s) and a method for Content Consumers to use to enforce the privacy consent appropriate to the use. This profile complements XDS by describing a mechanism whereby an XDS Affinity Domain can develop and implement multiple privacy policies, and describes how that mechanism can be integrated with the access control mechanisms supported by the XDS Actors.
Best Practice	The application of the best knowledge derived from accepted high quality research and respected expert experience to ensure NABIDH optimum processes and outcomes.
Breach	Any unauthorized access, disclosure, acquisition or use of Subject of care Data, whether by Wilful Misconduct or otherwise or any breach of DHA Policies. A Breach is a Reportable Event that, once investigated, is confirmed to have compromise the security or privacy of the Personal Health Information (PHI).
Break-Glass	Break the glass relates to an “emergency” and “temporary” authorization of a system user and is required to obtain access to information.

Term	Definition
Business Associate (BA)	A business associate is a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable Health Information .
Business Day	A day (other than a Friday, Saturday or public holiday) on which banks in the United Arab Emirates are generally open for normal business.
Clinical Vaccines Administered (CVX) code	Clinical Vaccines Administered (CVX) code is a numeric string, which represents the type of product used in an immunization. These codes are maintained by the Centers for Disease Control and Prevention, Immunization Information System Support Branch (IISSB) for use in HL7 data transmission. Every immunization that used a given type of product will have the same CVX, regardless of who received it. Typically, there are a number of factors that determine which vaccine will have the same or a different CVX code the formulation, the concentration, the manufacturing process (egg culture vs. cell culture), and the route of administration.
Competent Person	Refers to a person legally capable of consenting to be part of NABIDH includes every adult person, 18 years and above is assumed to be competent to consent, understand possible alternatives and consequences and uses that information in order to decide whether or not to participate in NABIDH unless ruled otherwise by the law of the UAE.
Confidentiality	Information is not made available or disclosed to unauthorized individuals, entities, or processes.
Consent	Is an agreement or permission accompanied by full information on the nature, risk and alternative of sharing Health Information through NABIDH. After receiving this information, the subject of care then either continue in NABIDH or refuses (e.g. opt out).

Term	Definition
Consistent Time Integration Profile (CT)	IHE-CT provides a means to ensure that the system clocks and time stamps of the many computers in a network are well synchronized. This profile specifies synchronization with a median error less than 1 second. This is sufficient for most purposes.
Credential	An object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person.
Cross-Community Access (XCA)	IHE- Cross-Community Access (XCA) profile supports the means to query and retrieve patient relevant medical data held by other communities. A community is defined as a coupling of facilities/enterprises that have agreed to work together using a common set of policies for the purpose of sharing clinical information via an established mechanism. Facilities/enterprises may host any type of healthcare application such as EHR, PHR, etc.
Cross-Community Patient Discovery (XCPD)	IHE- Cross-Community Patient Discovery (XCPD) supports the means to locate communities, which hold patient relevant health data and the translation of patient identifiers across communities holding the same patient's data.
Cross-Enterprise Document Sharing (XDS)	IHE- Cross-Enterprise Document Sharing (XDS) is focused on providing a standards-based specification for managing the sharing of documents between any healthcare enterprise, ranging from a private physician office to a clinic to an acute care in-patient facility and Electronic Medical Record (EMR) systems. XDS.b is the new profile of XDS.
Cross-Enterprise User Assertion Profile (XUA)	IHE- Cross-Enterprise User Assertion Profile (XUA) provides a means to communicate claims about the identity of an authenticated principal (user, application, system...) in transactions that cross enterprise boundaries. To provide accountability in these cross enterprise transactions there is a need to identify the requesting principal in a way that enables

Term	Definition
	the receiver to make access decisions and generate the proper audit entries.
Current Dental Terminology (CDT)	CDT is a code set with descriptive terms developed and updated by the American Dental Association (ADA) for reporting dental services and procedures to dental benefits plans. The purpose of the CDT Code is to achieve uniformity, consistency and specificity in accurately documenting dental treatment. One use of the CDT Code is to provide for the efficient processing of dental claims, and another is to populate an Electronic Health Record (EHR).
Current Procedural Terminology 4th Edition (CPT 4)	CPT 4 a numeric uniform coding system consisting of descriptive terms and identifying codes that are used primarily to identify medical services and procedures furnished by physicians and other healthcare professionals. CPT is currently identified by the Centers for Medicare and Medicaid Services (CMS) as Level 1 of the Healthcare Common Procedure Coding System. CPT code is maintained by the American Medical Association (AMA)
Data	Any data, including any health and other information, text, radiological images, laboratory results, medical reports, electronic claims and coding, drawings, health and other records, documents, and other materials which are embodied in any medium (including any electronic, optical, magnetic or tangible medium).
Data Integrity	Data that has not been altered or destroyed in an unauthorized manner.
Data Onboarding Requirements	The requirements that each Participant must comply with in making available Subject of care Data to the NABIDH Platform as published by NABIDH Operator from time to time.
Data Privacy and security officer	Is responsible for supervising the implementation of a data protection strategy ensuring it is compliant with NABIDH and other applicable data protection laws. This officer is ultimately responsible for both the data protection strategy and whomever they delegate operational duties to.

Term	Definition
Data Specification	The specifications detailing the content, format and technical and security requirements for Subject of care Data as published by the NABIDH Operator from time to time.
Data Supplier	An individual or entity that supplies Data to or through the NABIDH. Data Suppliers include both Participants and entities that supply to, but do not access Data through, the NABIDH (such as clinical laboratories and pharmacies).
Data Use Agreement	Comprehensive agreement that governs the exchange of health data between participants in NABIDH.
De-Identified Health Information/Data	Any Health Information or Subject of care Data that is 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.
Dubai Drug Code (DDC)	DDC List is a comprehensive list of all drugs that are registered with DHA's Pharmacy Services department. Each registered drug is assigned a unique DDC code allowing for differentiation between drugs as per the DDC structure which includes details such as route of administration (ROA), dosage, form, pack size, price, manufacturer, registered owner and source. Sources include MOH, DHA and Private Hospital. The Ministry of Health (MOH) and Dubai Health Authority (DHA) have unique codes established to code for drugs.
Dubai Scientific Research Ethics Committee (DSREC)	The DSREC is the central ethics committee in Dubai that facilitates the maintenance of ethical standards during the conduct of research. They also facilitate the understanding of the principle of scientific research including research design, analysis, and methodology. All medical and non- medical professionals from the Emirate of Dubai who wish to conduct research in the DHA and health facilities under the jurisdiction of DHA have to get approval from DSREC.
Electronic System	Software, portal, platform or other electronic medium controlled by a Healthcare Professional and/or a Healthcare Facility ,

Term	Definition
	through which they process or have the potential to process the Subject of care Data.
Emergency	A situation, which requires an immediate treatment/intervention to save a subject of care's life/limb or fetus or to remove hazards in order to prevent deterioration of the subject of care's condition, where the subject of care is not competent to consent and no next of kin, is available
Emergency Access	Access to data for the provision of care where threat of injury or death requires special permissions or override of other controls in order to ensure uninterrupted and urgent treatment.
Encounter	In relation to a subject of care, the period from when that Subject of care is first brought under the care of a Healthcare Professional at a Healthcare Facility until the time that Subject of care ceases to be under the care of a Healthcare Professional at that Healthcare Facility.
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.
Fast Healthcare Interoperability Resources (FHIR)	HL7 FHIR R4 is a next generation standards framework created by HL7. FHIR combines the best features of HL7's v2 , HL7 v3 and CDA product lines while leveraging the latest web standards: XML, JSON, HTTP, OAuth, etc., Support for RESTful architectures, seamless exchange of information using messages or documents, and service-based architectures and applying a tight focus on implementability. Fast Healthcare Interoperability Resources (FHIR) solutions are built from a set of modular components called "Resources". These resources can easily be assembled into working systems that solve real world clinical and administrative problems at a fraction of the price of existing alternatives. Fast Healthcare Interoperability Resources (FHIR) is suitable for use in a wide variety of contexts mobile phone apps, cloud communications, EHR-based data sharing, server communication in large institutional healthcare providers, and much more. Fast Healthcare Interoperability

Term	Definition
	Resources (FHIR) offers many improvements over existing standards.
Good clinical practice (GCP)	Good clinical practice is an international quality standard for conducting clinical trials that in some countries is provided by International Conference on Harmonization (ICH), an international body that defines a set of standards, which governments can then transpose into regulations for clinical trials involving human subjects.
Government Agency	Any agency, authority, board, commission, department, instrumentality, ministry, official, public person or statutory person of the United Arab Emirates or the Emirate of Dubai which, pursuant to Applicable Laws is entitled to regulate or influence the matters dealt with in this policy or the parties to this policy, as the case may be.
Government Oversight and Policy Task Force	Responsible for the implementation and enforcement of Policies and standards regarding the NABIDH's operations, infrastructure and data management to ensure accountability and a protection of Dubai's public interest and the individual's interest.
Health Information Exchange Nodes (HIE)	HIE nodes are those systems (Electronic Medical Records, Public Health Information Systems) that are connected to NABIDH.
Health Level Seven CDA Release 2.0 (HL7 CDA R2)	HL7 CDA R2 provides an exchange model for clinical documents (such as discharge summaries and progress notes) - and brings the healthcare industry closer to the realization of an electronic medical record. By leveraging the use of XML, the HL7 Reference Information Model (RIM) and coded vocabularies, the CDA makes documents both machine-readable - so they are easily parsed and processed electronically - and human-readable - so they can be easily retrieved and used by the people who need them. CDA documents can be displayed using XML-aware Web browsers or wireless applications such as cell phones. The product of 5 years of improvements, CDA R2 body is based on the HL7

Term	Definition
	Clinical Statement model, is fully RIM-compliant and capable of driving decision support and other sophisticated applications, while retaining the simple rendering of legally authenticated narrative.
Health Level Seven (HL7)'s Version 2.x (HL7 V2.x)	HL7 V2.x messaging standard is the workhorse of electronic data exchange in the clinical domain and arguably the most widely implemented standard for healthcare in the world. This messaging standard allows the exchange of clinical data between systems. It is designed to support a central patient care system as well as a more distributed environment where data resides in departmental systems. The HL7 V2.x Message Profiling informative document (2000) provides a guideline for documenting particular uses of HL7 messages. A defined V2.x message profile will be registered with HL7 and may be reused by other HL7 users, moving the HL7 V2.x standard closer to "plug and play" interfaces. With consistent and complete documentation, HL7 V2.x interface partners will explicitly understand what data will be passed, the format in which the data will be passed and, the acknowledgement responsibilities of the sender and receiver. Reduces implementation costs generally backward compatible.
Health Level Seven (HL7) Version 3 (V3)	HL7 V3 is the new generation differs that from V2 in that all standards developed under V3 arise from an underlying Reference Information Model (RIM), by applying a set of development steps defined in the HL7 Development Framework (HDF). The aim of V3 is to produce consistency in definition of different information objects and their representation in messages, thus allowing for easier implementation and the definition of clearer conformance requirements. Furthermore, the underlying modelling approach allows for the definition of standards for information representation other than just messages including forms, decision-support mechanisms and electronic patient record structures. HL7 V3 standards are developed as syntax-independent models. The current

Term	Definition
	preferred implementation technology is Extensible Mark-up Language (XML).
Health Record	Repository of information regarding the health of a subject of care. Under this policy, this refers to all personal Health Information accessible through the NABIDH Health Information Exchange.
Healthcare Common Procedure Coding System (HCPCS)	Healthcare Common Procedure Coding System (HCPCS) Level II is a set of healthcare procedure codes based on the American Medical Association's Current Procedural Terminology (CPT). Level II codes are maintained by the US Centers for Medicare and Medicaid Services (CMS). Level II of the HCPCS is a standardized coding system that is used primarily to identify products, supplies, and services not included in the CPT-4 codes, such as ambulance services and durable medical equipment, prosthetics, orthotics, and supplies (DMEPOS) when used outside a physician's office. The level II HCPCS codes were established for submitting claims for these items.
Healthcare Facility	A DHA licensed institution (including any hospital, clinic, surgery, pharmacy, diagnostic center, and other facility) where Healthcare services are provided by Healthcare Professionals in the Emirate of Dubai and has executed an effective Participation Agreement with the NABIDH Health Information Exchange.
Healthcare Operations	This includes, without limitation, administrative activities that support Health System Stakeholders, including conducting quality and improvement assessments; training employees; conducting medical, legal, and compliance reviews; performing audits; business planning and development; and other general management activities (e.g. customer service, resolving internal grievances, etc.).

Term	Definition
Healthcare Professional	A healthcare professional who treats or deals with subjects of care in the Emirate of Dubai who is licensed and regulated by DHA.
Identifier	Piece of information used to claim an identity, before a potential corroboration by a corresponding authenticator.
Immunization	The process whereby a person is made immune or resistant to an infectious disease. Typically, this is achieved by the administration of a vaccine. It is a proven tool for controlling and eliminating life threatening infectious diseases.
Incident	A security incident is an event that leads to a violation of an organization's security policies and puts sensitive data at risk of exposure.
Individuals	Individuals include healthcare providers, non-regulated health professionals, researchers, subjects of care, and subject of care agents.
Information and Communication Technology (ICT) Law	UAE Federal Law No.(2) For the Year 2019 on the use of Information and Communication Technology (ICT) in healthcare.
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.
Information System	An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.
Insolvency Event , In respect of a Participant	(a) if that Participant has any distress or execution levied or enforced on any of its assets which is not paid out within 7 days of it being levied

Term	Definition
	(b) if that Participant calls a meeting for the purpose of passing a resolution to wind it up, or such a resolution is passed, save in respect of such resolution being proposed for the purposes of a bona fide company reorganization (c) if that Participant presents, or has presented, a petition for a winding up order (d) an application to appoint an administrator is made in respect of that Participant or a notice of intention to appoint an administrator is filed in respect of that Participant (e) any other steps are taken by that Participant or any other person to appoint an administrator over that Participant (f) if that Participant has an administrator, administrative receiver, or receiver appointed over all or any part of its business, undertaking, property or assets (g) if that Participant takes any steps in connection with proposing a company voluntary arrangement or a company voluntary arrangement is passed in relation to the arrangement (h) If that Participant ceases, or appears in the reasonable opinion of NABIDH Operator likely or is threatening to cease to trade (i) If that Participant stops or suspends making payments (whether of principal or interest) with respect to all or any class of its debts or announces an intention to do so or that Participant suspends or ceases or threatens to suspend or cease to carry on its business; and/or (j) If that Participant suffers or undergoes any procedure analogous to any of those specified above or any other procedure available in the country in which that Party is constituted, established or domiciled against or to an insolvent debtor or available to the creditors of such a debtor.

Term	Definition
Institutional Review Board (IRB)	An institutional review board (IRB), also known as an independent ethics committee (IEC), ethical review board (ERB), or research ethics board (REB), is a type of committee that applies research ethics by reviewing the methods proposed for research to ensure that they are ethical. Such boards are formally designated to approve (or reject), monitor, and review biomedical and behavioral research involving humans. They often conduct some form of risk-benefit analysis in an attempt to determine whether or not research should be conducted. The purpose of the IRB is to assure that appropriate steps are taken to protect the rights and welfare of humans participating as subjects in a research study.
Insured Subject of care	Any individual who is insured for healthcare services in the Emirate of Dubai by a Payer.
Insured Subject of care Data	Data relating to an Encounter with that Insured subject of care that is made available to the NABIDH Platform by each Healthcare Facility that provides healthcare services to that Insured subject of care from time to time in accordance with the requirements and timeframes of the Applicable Laws issued, brought into effect and maintained by DHA regarding the generation, compilation, processing, supply and use of such Data.
Integrity	The properties of the Data have not been altered or destroyed in an unauthorized manner.
International Classification of Diseases, Tenth Revision, and Clinical Modification (ICD-10-CM)	ICD-10-CM is a morbidity classification published by the Centers for Medicare and Medicaid Services (CMS) and the National Center for Health Statistics (NCHS). ICD-10-CM is a system used by physicians and other healthcare providers to classify and code all diagnoses, symptoms and procedures recorded in conjunction with hospital care. It provides a level of detail that is necessary for diagnostic specificity and morbidity classification.

Term	Definition
International Council for Harmonization (ICH)	The International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use.
International Refined Diagnosis Related Groups (IR-DRGs)	IR-DRG The Dubai Health Authority (DHA) has adopted for inpatient hospital payment. Each inpatient hospital stay is assigned to one and only one IR-DRG based on the patient's age, sex, diagnoses, procedures provided to the patient, and sometimes other factors. The hospital services included in each IR-DRG bundle represents the typical services provided across all hospitals for inpatients with similar reasons for admission.
Interoperability	The interfacing of the NABIDH with the Electronic Systems of each Participant, such that the Data provided by one institution can meaningfully be used by another to improve quality and coordination of care.
key performance indicators (KPIs)	The key performance indicators to be agreed and developed between the NABIDH Operator and the DHA.
Launch Schedule	Required onboarding date for Healthcare Facilities to the NABIDH Platform assigned by the NABIDH Operator.
Law	Law means a local or federal constitution, decree, regulation, rule, bylaw, or other governmental action having the force and effect of law.
Logical Observation Identifiers Names and Codes (LOINC)	LOINC is a standard for identifying medical laboratory observations. It was created by the Regenstrief Institute Inc., LOINC is a common language (a set of identifiers, names, and codes) for identifying health measurements, observations, and documents. LOINC is a rich catalogue of measurements, including laboratory tests, clinical measures like vital signs and anthropometric measures, standardized survey instruments, and more.
Malicious Software	Any software, virus, Trojan horse, time bomb or other code (which can take the form of but not limited to Java applets,

Term	Definition
	ActiveX controls, scripting languages, browser plug-ins or pushed content) that is harmful, disabling or which is designed to permit or enable a breach or unauthorized access to the NABIDH Platform or subject of care data or theft or damage to the NABIDH platform or subject of care data or otherwise impairs the operation of the NABIDH Platform or the ability to transact subject of care data.
Minor	If the subject of care is below 18 years.
NABIDH	NABIDH stands for "Network and Analysis Backbone for Integrated Dubai Health". NABIDH is DHA's Health Information Exchange (NABIDH) solution. NABIDH allows doctors, nurses, pharmacists, other health care providers and subject of cares to appropriately access and securely share a subject of care's vital medical information electronically—improving the speed, quality, safety and cost of subject of care.
Non-Competent Person	Refers to subject of care's lack of legal capacity or subject of care has full capacity , but it is not possible to obtain consents due to of any of the following circumstances: (a) Unconscious or has altered perception due to mental or psychological disease (b) Health condition does not allow taking his/her approval
Non-Regulated Health Professional	Person employed by a healthcare organization who is not a regulated health professional. Examples: Medical receptionist who organizes appointments or a nurse's aide who assists with subject of care service.
"Normalized" notations for clinical drugs (RxNorm)	RxNorm is a catalogue of the standard names given to clinical drugs and drug delivery devices to enable interoperability and clear communication between electronic systems, regardless of software and hardware compatibility. RxNorm is part of Unified Medical Language System (UMLS) terminology and is maintained by the United States National Library of Medicine

Term	Definition
	(NLM). RxNorm Provides information about all the registered drugs in GCC and Middle East such as drug to drug reactions, drug to allergy interaction, high dose , low dose etc.,.
Participant	An entity or person who enters into the Participant Agreement on behalf of one or more Healthcare Facilities, which authorizes those Healthcare Facilities and their respective Healthcare Personnel to access, use or receive services via, or supply Data to, the NABIDH Platform.
Participant Agreement	The agreement made by and between the NABIDH Operator and each Participant, which sets forth the terms and conditions governing the operation of the NABIDH Platform and the rights and responsibilities of the Participants and the NABIDH with respect to the NABIDH Platform.
Participant Personnel	Any person employed or engaged by a Participant and/or any of its sub-contractors or who was at any time so employed or engaged in relation to NABIDH Platform. Participant System: In relation to each Participant, the software, hardware, portal, database, platform or other electronic medium controlled by the Participant (Irrespective of whether it is owned, leased, licensed or operated by or on behalf of that Participant) and used to process subject of care data and interface with the NABIDH platform.
Participation Criteria	The criteria specified by NABIDH Operator from time to time, DHA Policies, the NABIDH Platform Interface Standards, the NABIDH Platform Access Requirements, Data Specifications and the Data Onboarding Requirements.
Parties	NABIDH Operator and each Participant, and 'Party' shall be construed accordingly.
Patient Identifier Cross Referencing (PIX)	IHE-PIX Integration Profile supports the cross-referencing of patient identifiers from multiple Patient Identifier Domains by Transmitting patient identity information from an identity source to the Patient Identifier Cross-reference Manager and providing

Term	Definition
	the ability to access the list(s) of cross-referenced patient identifiers either via a query/ response or via an update notification.
Personal Health Information (PHI)	Any Subject of care data, including any health and other information, text, radiological images, laboratory results, medical reports, electronic claims and coding, drawings, health and other records, documents and other materials which are embodied in any medium (including any electronic, optical, magnetic or tangible medium). This would include any oral or recorded information relating to the past, present, or future physical or mental health of a subject of care the provision of health care to the subject of care, or the payment for health care.
Personal Representatives	A person who manages the legal affairs of another because of incapacity or death.
Policies	Refer to decisions, plans, and actions that are undertaken to NABIDH DHA's health care goals for Dubai. DHA's policies define a vision for the future, which in turn helps to establish targets and points of reference for the short and medium term. They outline priorities and the expected roles of different groups, and it builds consensus and informs people. For the purposes of this policy, references to the Policies includes all Applicable Laws.
Portal	Web access channel to Health Information Exchange. This may be a Provider Portal supporting the HEALTHCARE FACILITY or a Client Portal supporting the Subject of Care.
Principal Investigator (PI)	Principal Investigator (PI) is the primary individual responsible for the preparation, conduct, and administration of a research grant, cooperative agreement, training or public service project, contract, or other sponsored project in compliance with applicable laws and regulations and institutional policy governing the conduct of research.

Term	Definition
Principle of Minimal Privilege (POMP)	The principle of minimal privilege also known as the principle of least authority (POLA), is the idea that at any user, program, or process should have only the bare minimum privileges necessary to perform its function
Privacy	Freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual. In the context of the NABIDH, it refers to an individual's interest in limiting who has access to personal healthcare information.
Processing	Any operation or set of operations which is performed upon Subject of care Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use or disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction and processed, processes and process shall be construed accordingly
Regulated Health Professional	Shall mean healthcare personnel working in health facilities and required to be licensed as per the applicable laws in the United Arab Emirates
Remote Access	Access to the NABIDH Health Information Exchange from a device connected to a NABIDH node and situated outside of the physical and environmental control of the corresponding Healthcare Facility. This would typically include access to a NABIDH node from a remote location such as from home.
Reportable Event	A Reportable Event is an action (or lack of action), suspected or confirmed, that violates NABIDH policies and procedures for accessing or using Health Information managed by the NABIDH Health Information Exchange. Such violations may be unintentional or intentional.
Research	Is an original investigation undertaken in order to contribute to knowledge and understanding.

Term	Definition
Research Ethics	Research that involves human subjects or participants raises unique and complex ethical, legal, social and political issues. Research ethics is specifically interested in the analysis of ethical issues that are raised when people are involved as participants in research. There are three objectives in research ethics. The first and broadest objective is to protect human participants. The second objective is to ensure that research is conducted in a way that serves interests of individuals, groups and/or society as a whole. Finally, the third objective is to examine specific research activities and projects for their ethical soundness, looking at issues such as the management of risk, protection of confidentiality and the process of informed consent.
Risk	The quantifiable likelihood of potential harm that may arise from a future event.
Risk Assessment	The process used to determine risk management priorities by evaluating and comparing the level of risk against predetermined standards, target risk levels, or other criteria.
Role	Set of competences and/or performances that are associated with a task.
Secondary use of personal data (Repurposing data)	Secondary use of personal data is any use different from primary use. NOTE: For example, the primary use is for treating the individual subject of care; we can consider that the secondary use is for purposes other than treating the individual subject of care, such as for research or marketing.
Security	Combination of availability, confidentiality, integrity, and accountability.
Security audit	An independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policies and operational

Term	Definition
	procedures, to detect security breaches and to recommend any indicated changes in control policy and procedures.
Sensitive Health Information	Special categories of Health Information as identified by NABIDH Operator that require additional restrictions on disclosure and use as determined by NABIDH Operator from time to time, which may include information regarding: (a) Any Very Important Person (VIP) Subject of care (which includes but is not limited to any VIP Subject of care Data) (b) Chemical dependency (c) Human immunodeficiency virus (HIV), also known as Acquired Immune Deficiency Syndrome (AIDS)/HIV/ AIDS status (d) Mental health conditions (e) Behavioral Health Information (f) Psychotherapy Notes (g) Alcohol and substance abuse (h) Reproductive health (i) Genetic testing information (j) Sexual health (including sexually transmitted diseases). (k) Child pregnancy data (l) Child abuse conditions
Subject of Care	Person who receives health related services and has Health Information contained within the NABIDH; any person who uses or is a potential user of a healthcare service; subjects of care may also be referred to as subject of cares, healthcare consumers or Subjects of Care.
Subject of Care Agent	Parent, guardian, or other legal representative of the subject of care.
Subject of care Data	In relation to each individual who receives healthcare services in the Emirate of Dubai and data (including but not limited to medical records) relating to each Encounter with that individual

Term	Definition
	that resides and is processed on a participant's system in accordance with the Participant Agreement and the Policies.
Subscriber	A party who receives a credential or token from a certification service provider.
System Access	The ability or authority to interact with the NABIDH Platform; a means by which one may input or output data from the NABIDH Platform. Access requires authorization and proper clearance in accordance with Polices and the Participation Criteria.
Systematized Nomenclature of Medicine - Clinical Terms (SNOMED CT)	SNOMED CT is a systematically organized computer processable collection of medical terms providing codes, terms, synonyms and definitions used in clinical documentation and reporting. It is considered to be the most comprehensive, multilingual clinical healthcare terminology in the world. A resource with comprehensive, scientifically validated clinical content, enables consistent representation of clinical content in electronic health records. SNOMED CT is maintained and distributed by SNOMED International. SNOMED International is the trading name of the International Health Terminology Standards Development Organisation (IHTSDO).
Third Party	Each person or entity, which is not a Party to the Participant Agreement.
Threat	Is the expressed potential for the occurrence of a harmful event such as an attack. It could be any party with the intent and capability to exploit vulnerability in an asset such as a malicious hacker or a disgruntled employee.
Transact	To send, supply, submit, route, make available to, upload, request, receive, respond to or publish Subject of care data via the NABIDH Platform and 'Transacted' and 'Transaction' shall be construed accordingly.

Term	Definition
Universal Numbering System (UNS)	UNS is a tooth notation system and has been adopted by the American Dental Association (ADA) and it is in use by most general dentists. Teeth are numbered from the viewpoint of the dental practitioner looking into the open mouth, clockwise starting from the distal most right maxillary teeth.
Very Important Person (VIP) Subject of care	A Subject of care identified by the NABIDH Operator as a VIP who receives or has received healthcare services in the Emirate of Dubai and in respect of whom there are increased levels of control over access to that subject of care's data.
Very Important Person (VIP) Criteria	(a) Senior visitors (leaders and heads of state) (b) Foreign ministers during their visit to the UAE (c) Ambassadors and Delegates in the UAE (d) Ministers and Undersecretaries of the Ministry of the UAE (e) Chairmen and Undersecretaries of the government departments of the UAE (f) Royals and crown princes of the UAE and other Emirates including their immediate family members (wives, sons, daughters, brothers and sisters) (g) Al Nahyan and Al Maktoum family members (h) Members with prefix “Sheikh” or “Sheikha” in their official identity (i) Members with prefix “High Excellence” or “Her Excellence” in their official identity.
Vulnerability	Vulnerability Is weakness in an asset that can be exploited.
Workstation	An electronic computing device, for example, a laptop or desk computer, or any other device that performs similar functions and electronic media stored in its immediate environment.

Table 1: Definitions

5. ABBREVIATIONS

AAC	:	Authentication and Access Control
ACL	:	Access Control List
ADA	:	American Dental Association
ADM	:	Administration
AES	:	Advanced Encryption Standard
AMA	:	American Medical Association
APM	:	Authentication and Password Management
ASCII	:	American Standard Code for Information Interchange
ASLR	:	Address Space Layout Randomization
CA	:	Certificate Authority
CAPTCHA	:	Completely Automated Public Turing test to tell Computers And Humans Apart
CDT	:	Current Dental Terminology
CMMS	:	Centers for Medicare and Medicaid Services
CPT	:	Current Procedural Terminology 4th Edition
CRP	:	Cryptography
CS	:	Code Security
CSP	:	Cloud Service Provider
CSPRNG	:	Cryptographically Secure Pseudorandom Number Generator
CSS	:	Cascading Style Sheets
CVX	:	Clinical Vaccines Administered
DBM	:	Database Management
DDC	:	Dubai Drug Code
DEP	:	Deployment
DHA	:	Dubai Health Authority
DI	:	Data Integrity
DSP	:	Data Storage & Protection
EBMD	:	Electronic Bio-Medical Devices
EH	:	Exception Handling
EHR	:	Electronic Health Record
EMR	:	Electronic Medical Record

EPHI	:	Electronic protected health Information
FA	:	Functional Architecture
FHIR	:	Fast Healthcare Interoperability Resources
GUD	:	Guideline
HCPCS	:	Healthcare Common Procedure Coding System
HIE	:	Health Information Exchange
HISHD	:	Health Informatics and Smart Health Department
HISS	:	DHA Health Information Security Standard
HL7	:	Health Level Seven International
HRS	:	Health Regulation Sector
HTML	:	Hypertext Mark-up Language
HTTP	:	Hypertext Transfer Protocol
HTTPS	:	Secure Hypertext Transfer Protocol
ICD-10-CM	:	International Classification of Diseases, Tenth Revision, Clinical Modification
ICT	:	Information and Communication Technology
IHE	:	Integrating the Healthcare Enterprise
IHE-ATNA	:	Audit Trail and Node Authentication Integration Profile
IHE-BPPC	:	Basic Subject of care Privacy Consents Integration Profile
IHE-CT	:	Consistent Time Integration Profile
IHE-PDQ	:	Subject of care Demographics Query Integration Profile
IHE-PIX	:	Subject of care Identifier Cross Referencing Integration Profile
IHE-XCA	:	Cross-Community Access Integration Profile
IHE-XCPD	:	Cross Community Subject of care Discovery Integration Profile
IHE-XDS	:	Cross-Enterprise Document Sharing Integration Profile
IHE-XUA	:	Cross-Enterprise User Assertion Integration Profile
IHTSDO	:	International Health Terminology Standards Development Organisation
IISSB	:	Immunization Information System Support Branch
IR-DRG	:	International Refined Diagnosis Related Groups
IT	:	Information Technology
IV	:	Input Validation
LDAP	:	Lightweight Directory Access Protocol
LEG	:	Legislations

LM	:	Logging and Monitoring
LOINC	:	Logical Observation Identifiers Names and Codes
MAC	:	Media access control address
MGUD	:	Mobile Development Guideline
MPTD	:	Mobile Application Provisioning/testing/distribution
NABIDH	:	Health Information Exchange in the Emirate of Dubai
NCHS	:	National Center for Health Statistics
NEMA	:	National Electrical Manufacturers Association
NIST	:	National Institute of Standards and Technology
NLM	:	National Library of Medicine
PHI	:	Personal Health Information
PII	:	Personally Identifiable Information
PM	:	Password Management
QA	:	Quality Assurance
RI	:	Regenstrief Institute Inc.
RIM	:	Reference Information Model
ROA	:	Route of Administration
RSA	:	Rivest-Shamir-Adleman
RxNorm	:	Normalized notations for clinical drugs
SEC	:	Security
SFTP	:	SSH File Transfer Protocol
SHA	:	Secure Hash Algorithm
SM	:	Session Management
SNOMED CT	:	Systematized Nomenclature of Medicine - Clinical Terms
SQL	:	Structured Query Language
SSH	:	Secure Shell
SSL	:	Secure Sockets Layer
UAE	:	United Arab Emirates
UMLS	:	Unified Medical Language System
UNS	:	Universal Numbering System
URL	:	Uniform Resource Locator
UTF-8	:	Unicode Transformation Format

6. BACKGROUND

NABIDH's Health Information Exchange and Population Health Program will create a combined public and private healthcare platform that unifies subject of care data into one unique record. Through the NABIDH program DHA and non-DHA healthcare providers can view subject of care data through a dedicated, secure portal. In addition, Dubai's citizens and residents can access their healthcare data from all medical facilities in Dubai. Nabidh will give the privilege of accessing population health insights to drive higher standards in preventative care.

Currently, personal Health Information is not utilized to its full potential to support effective and efficient care due to fragmented information creation and storage. Health Information systems are typically isolated, within hospitals, physician practices, laboratories, or pharmacies. Changes in insurance coverage, reliance on multiple providers, and increases in specialty care add more and more potentially relevant, but disparate, information into a fragmented, non-interoperable non-system.

Several factors mandate having solo HIE platform in the Emirate of Dubai. Natural disasters displace individuals to locales with unfamiliar providers and can destroy or render inaccessible existing Health Information repositories. The growing use of pharmaceuticals and associated recalls of drugs from the market may call for immediate identification of affected individuals. Finally, the likelihood of serious pandemics calls for rapid identification of ill persons and accurate immunization histories.

Policy makers, researchers, industry groups, and healthcare professionals identify HIE as a solution to these problems. Health Information Exchange is the process of sharing subject of care-level electronic Health Information between different

organizations, the potential effects of making previously unavailable subject of care-level information available to healthcare professionals are widespread and address nearly all of the Institute of Medicine's quality aims. While HIE promises cost and quality improvements, to date we lack substantial and consistent comprehensive medical record for individuals.

This document defines the HIE policies and standards that need to exist (created or updated) in order to successfully launch NABIDH.

7. The HIE Policies and Standards Framework

The purpose of this document is to facilitate data privacy, health information protection and security measures for the implementation of NABIDH across public and private healthcare facilities in Dubai. In addition, we are providing the necessary standards that healthcare facilities need to follow/ maintain in order to join the NABIDH HIE platform.

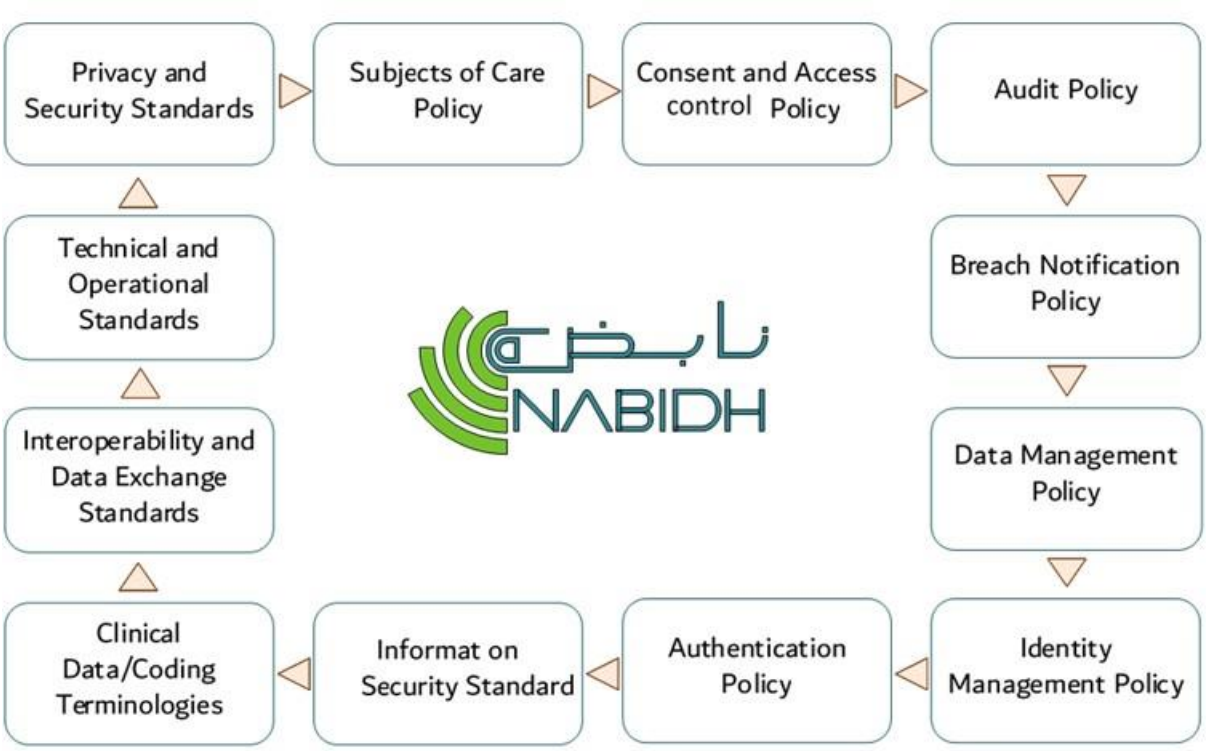

Figure 1: The HIE Policies and Standards Framework

The details of these policies and standards themes are highlighted below:

- **Subject of Care Policy:** The purpose of this policy is to define Subjects of Care and healthcare consumer expectations that will govern the design and implementation of NABIDH.
- **Consent and Access Control Policy:** This policy defines who and how individuals and systems can access NABIDH managed data. This policy also defines the circumstances in which a Subject of Care can permit or withhold the use and disclosure of NABIDH accessible Health Information.
- **Incident Management and Breach Notification policy:** This policy is to define policy surrounding identification, investigation, notification, and mitigation of a breach within NABIDH system.
- **Audit Policy:** This policy is to ensure that the security and confidentiality of Subject of Care data transmitted through NABIDH are monitored/tracked through privacy/security audits.
- **Data Management and Quality Policy:** This policy is to define policy surrounding primary and secondary use of data that includes acquiring, validating, storing, protecting, and processing required data to ensure the accessibility, reliability, and timeliness of the data for its users.
- **Identity Management Policy:** This policy ensures that systems and individuals interacting with NABIDH are known through the process of reliable security identification of subjects by incorporating an identifier and its authenticator.

- **Authentication Policy:** This policy ensures that systems and individuals interacting with NABIDH are known through the process of reliable security identification of subjects by incorporating an identifier and its authenticator.
- **Information Security Standards:** This standard ensures that all information technology users within the organization or its networks comply with rules and guidelines related to the security of the information stored digitally at any point in the network.
- **Clinical Data Coding Terminologies:** Terminology standards is structured collection of medical terms for recording and coding of clinical information that is computer processable thereby reducing the variability in the way clinical data is captured, encoded and stored.
- **Interoperability and Data Exchange Standards:** Messaging standards allows the exchange of clinical data between systems as per published specifications. It is designed to support a central subject of care system as well as a more distributed environment where data resides in multiple ancillary and departmental systems.
- **Technical and Operational Standards:** Technical and Operational standards would be used for integration of different systems and shall be used for communication in a safe and secure manner.

8. PURPOSE

8.1. To align with the Dubai Health Authority (DHA) vision, mission and strategic objective in improving the health service in the Emirate of Dubai.

8.2. To ensure that all Healthcare Stakeholders can actively participate in and benefit from the meaningful and secure exchange of Health Information.

9. SCOPE

The policies and procedures described in this document (NABIDH Policies and Standards) apply to all Participants and Authorized Users accessing the NABIDH HIE. This document is intended to ensure that the NABIDH is used in an effective, efficient, ethical, and lawful manner. The authorized users are:

9.1. Healthcare Facilities.

9.2. Business Associates of Healthcare Facilities.

9.3. Any subcontractors of Business Associates that perform functions or provide services involving the use and disclosure of PHI.

9.4. Any NABIDH Service Provider,

9.5. Any other subcontractor of the NABIDH platform.

10. APPLICABILITY

These policies and standards apply to the NABIDH platforms, and to all individuals and organizations that have access to NABIDH managed health records, including:

10.1. Healthcare Facilities.

10.2. Healthcare Facilities business associates.

10.3. Any subcontractors of business associates that perform functions or provide services involving the use and disclosure of PHI.

10.4. Any NABIDH platform Systems Service Provider.

10.5. Any other subcontractor of NABIDH platforms.

10.6. This policy applies to all personal Health Information provided to or retrieved from NABIDH platform.

11. SECTION 1: Subject of Care Rights

11.1. Purpose:

11.1.1. To inform the Subject of Care of their rights and role in the Nabidh platform.

11.1.2. To define Subject of Care expectations from NABIDH system.

11.1.3. To provide the Subject of Care the highest quality of care possible using NABIDH.

11.1.4. To encourage maximum number of participants in NABIDH program and allowing providers and government to continuously make improvements to the system of care.

11.2. Scope/Applicability

This policy applies to all healthcare facilities involved in the protection of Personal Health Information (PHI) including:

11.2.1. DHA and their Business Associates or any subcontractors, who is responsible for oversight of NABIDH platform.

11.2.2. NABIDH and their Business Associates or any subcontractors who is responsible for exchange of PHI.

11.2.3. Healthcare Facilities Their Business Associates or any subcontractors who is responsible for submission, collection and use of PHI.

11.2.4. Subject of Care or the Subject of Care Agent who is responsible for providing appropriate consent to their PHI.

11.3. Policy Statement:

11.3.1. Dubai Health Authority shall:

11.3.1.1. Oversee the implementation of policies, standards, and guidelines related to NABIDH participation as necessary in accordance with all Applicable Laws and DHA regulations.

11.3.1.2. Monitor on compliance with the NABIDH policies.

11.3.2. NABIDH Platform shall:

11.3.2.1 Maintain privacy and security protocols (physical, administrative, and technological) that are compliant with Applicable Laws.

11.3.2.2 Make all efforts to implement and maintain systems for Health Information Exchange that protect the integrity, security, privacy, and confidentiality of a Subject of Care's information.

11.3.2.3 Make information available to Subjects of Care regarding how their PHI could be used, who could have access to it, and under what circumstances it could be disclosed.

11.3.2.4 Make all efforts to assure identity of the Subject of Care is scrutinized in accordance with the NABIDH identity Management Policy for all Subject of Care accessible Health Information services.

11.3.2.5 Implement education programs to promote awareness on:

a. The value of the NABIDH.
b. How the NABIDH will operate.
c. What information will or will not be available on the NABIDH.
d. NABIDH privacy and security protections.
e. How to participate in NABIDH and the Subject of Care rights.
f. Benefits and remedies afforded to Subject of Care.

11.3.2.6 Be responsible for Health service management and quality assurance.

11.3.2.7 Implement and publish NABIDH governance structure that shall be transparent.

11.3.2.8 Subject of care Health Information will be shared with Healthcare Facilities unless the Subject of Care opts out of the NABIDH or specific Healthcare Facilities.

11.3.3. <u>All Healthcare Facilities shall</u>:

11.3.3.1 Comply with relevant DHA regulatory requirements regarding subject of care rights and responsibilities.

11.3.3.2 Make all efforts that each Subject of Care shall receive information at the Subject of Care's first visit following the provider's participation as a NABIDH Healthcare Facilities.

11.3.3.3 Provide information to Subject of Care at least once (e.g. in the entrance of a care facility, on a facility website, or when providing an account to the consumer portal).

11.3.3.4 Provided information to Subject of Care should be concise, transparent, intelligible, easily accessible, and uses clear and plain language.

11.3.3.5 Provide information about the procedure to opt out from the NABIDH.

11.3.3.6 Provide informative materials to Subject of Care regarding NABIDH platform and materials should minimally include Information regarding:

a. Purpose of the Health Information exchange.
b. Benefits.
c. How Health Information are protected.
d. How Health Information can be used.
e. Retention period of Health Information.
f. Contact information to the NABIDH to obtain more information.

11.3.3.7 Make information available to Subjects of Care regarding how their Health Information could be used, who could have access to it, and under what circumstances it could be disclosed.

11.3.3.8 Provide significant education program so that individuals understand how the NABIDH will operate, what information will or will not be available on the NABIDH, the value of the NABIDH, its privacy and security protections, how to participate in the exchange and the rights, benefits and

remedies afforded to them and how to access subject of care portal.

11.3.4. The Subject of Care or the Subject of Care Agent shall:

11.3.4.1 Be able to access their relevant PHI contained within the NABIDH in a readable form and format including an electronic format.

11.3.4.2 Subject of care Health Information should be available to the Subject of Care conveniently.

11.3.4.3 Subject of care Health Information shall be available to the Subject of Care affordably.

11.3.4.4 The Subject of Care shall have provision to upload clinical/ laboratory documents into NABIDH through portal for the treatment received from other healthcare providers outside Emirate of Dubai and UAE.

11.3.4.5 Subject of Care shall be responsible for uploading the correct clinical/laboratory documents and information on the portal for the treatment received from other healthcare providers outside Emirate of Dubai and UAE.

11.3.4.6 Subjects of care should have a means of direct, secure access to their relevant PHI that does not require physician or institutional mediation (Example: Through Subject of care Portal or through other approved services).

11.3.4.7 Subjects of Care shall be able to supplement their PHI without fees or burdensome processes.

11.3.4.8 Rights and process for complaints if the Subject of Care suspects a breach should be clear. Refer to complaints process in reference section of this manual.

11.3.4.9 In the case of a suspected breach, the Subject of Care that is the data subject of such a breach may request an investigation (refer to Breach Notification Policy). Such a request shall be issued by the Subject of Care or by the authorized Subject of Care agent; should the Subject of Care be unable to do so.

11.3.4.10 Such requests shall be directed to the Data Privacy and Security Officer / Health Information Management Personnel within the suspected Healthcare Facility and NABIDH designated team.

11.3.4.11 In the case of a breach identified and investigated through the NABIDH, the Subject of Care that is the data subject of such a breach will be notified.

11.3.4.12 Subject of Care should have the right to request a report of electronic disclosures for information accessed through the NABIDH where the Subject of Care is the data subject.

11.3.4.13 Such a request shall be issued by the Subject of Care or by the authorized Subject of Care agent should the Subject of Care be unable to do so,

11.3.4.14 The request shall be directed to the local Data Privacy and Security Officer, HISHD, or NABIDH designated team.

11.3.4.15 Report of electronic disclosures shall include information such as:

a. Date of disclosure.
b. Name of the Healthcare facility or person that received the disclosure.
c. Name of the Healthcare facility or person that made the disclosure.

11.3.4.16 The Subject of Care should be provided notification of break-glass accesses to his/her Subject of care Health Information through appropriate means such as email, cell phone etc.

11.3.4.17 The Subject of Care may choose to opt out of the NABIDH. In order to exercise this option, the Subject of Care shall follow the op out procedure provided by Healthcare Facility. Procedures and instructions for how to opt out of the NABIDH shall be provided to the Subject of Care or to the authorized Subject of Care agent should the Subject of Care be unable to review or comprehend the instructions.

11.3.4.18 All opt out requests shall be issued by the Subject of Care or by the authorized Subject of Care agent in the event that the Subject of Care is unable to do so. The healthcare provider may process the request on behalf of the Subject of Care.

11.3.4.19 The Subject of Care may choose to opt back in to the NABIDH at any time as per NABIDH process.

12. SECTION 2: Consent and Access Control

12.1. Purpose:

14.1.1. The purpose of this policy is to ensure accessing and sharing of PHI shall comply with all applicable UAE laws and DHA regulations.

14.1.2. This policy ensures that the Subject of Care or his / her agent understands and agrees to the sharing of PHI as well as the risks, benefits and alternatives.

14.1.3. This policy also defines the circumstances in which a Subject of Care can permit or withhold the use and disclosure of NABIDH accessible PHI.

14.1.4. Subject of care can be a UAE national, resident of UAE, or a Tourist.

12.2. Scope/Applicability:

This policy applies to everyone involved in the protection of PHI including:

14.2.1. DHA and their Business Associates or any subcontractors, who are responsible for oversight of NABIDH platform.

14.2.2. NABIDH and their Business Associates or any subcontractors who are responsible for exchange of Subject of Care PHI.

14.2.3. Healthcare Facilities and their Business Associates or any subcontractors who are responsible for submission, collection and use of Subject of Care PHI.

14.2.4. Subject of Care or the Subject of Care Agent who is responsible for providing appropriate consent to their PHI.

12.3. Policy Statement:

12.3.1. Dubai Health Authority shall:

12.3.1.1. Authorize Healthcare Facility to share and receive PHI through NABIDH.

12.3.1.2. Require Healthcare Facilities to obtain Subject of Care consent for sharing of PHI (both legacy and new data) via NABIDH in accordance with all applicable UAE laws and DHA regulations.

12.3.2. NABIDH shall:

12.3.2.1. Comply with DHA's mandate to share Subject of Care legacy and new PHI with Healthcare Facility.

12.3.2.2. Impose suitable measures on Healthcare Facility in order to prevent Very Important Person (VIP) Subject of care PHI from being exchanged or stored on the NABIDH Platform except in accordance with the directions of the DHA and as set out in the Participation Criteria if any.

12.3.2.3. Define Specific PHI that shall be made available by each Healthcare Facility.

12.3.2.4. Send circulars to Healthcare Facility to mandatorily capture subject of care address including the Emirate ID, name, and address. In addition to identify if the subject of care is a Tourist.

12.3.2.5. In the case where the Subject of Care has Opted Out of NABIDH then:

a. Personal Health Information shall continue to be received by NABIDH from Healthcare Facility.
b. Subject of care identifiers shall be anonymized.
c. Clinical data shall be stored without anonymization.
d. Personal Health Information shall not be retrieved using break glass.

12.3.2.6. Verify and provide access to NABIDH Clinician portal to manage Health Information consent according to all applicable UAE laws and DHA regulations (Example: Subject of care provider relationship, through application programming interfaces (API), etc.).

12.3.2.7. Ensure systems providing access to information/documents enforce protections associated with content marked as sensitive data:

a. Sensitive Health Information shall be restricted to care providers as identified by their role.
b. Sensitive Health Information shall be flagged to the care providers through special Icons, different color etc.
c. Sensitive Health Information may be accessed with a “break glass” option for defined roles of health professionals as

identified by NABIDH, which will trigger notification to the subject of care and Data Security and Privacy Officer, and after-the-fact review in accordance with the NABIDH Audit Policy (Section 4).

12.3.2.8. Ensure that all NABIDH individual users are associated with at least one standard healthcare role:

a. Administrative personnel should only access administrative information.
b. Clinical information is restricted to Healthcare professionals, defined by a set of roles in NABIDH authentication policy.
c. For Regulated Health Professional, the role shall be defined by the role code associated with the license as maintained by DHA Sheryan.
d. For Non-Regulated Health Professional, the role shall reflect one of the standard roles identified by NABIDH as determined by the Healthcare Facility responsible for the user's interactions with NABIDH system.

12.3.2.9. NABIDH will receive consent related requests from Healthcare Facility and will manage appropriately.

12.3.3. Healthcare Facilities shall:

12.3.3.1. Inform Subject of Care appropriately that sharing relevant PHI with NABIDH is part of their treatment through consent process.

12.3.3.2. Inform and initiate registration process of the Subject of care on the NABIDH subject of care portal registration.

12.3.3.3. Record the consent process in NABIDH when a Subject of Care chooses to Opt Out or opt in of the NABIDH.

12.3.3.4. Capture all mandatory demographics information required to support consent management process to Subject of Care (Emirates ID, Home address, Mobile number, etc.); and categorize subject of care if they are Tourists.

12.3.3.5. Implement necessary internal policies and procedures to prohibit sharing VIP Subject of care Health Information to the NABIDH Platform, except in accordance with the requirements of DHA or as set out in the Participation Criteria if any.

12.3.3.6. Establish organization policies to assure compliance with NABIDH policies. These policies are subject to review and audit in accordance with the NABIDH Audit Policy.

12.3.3.7. Ensure all relevant information flows to NABIDH, except where laws or policies of the Healthcare Facility prohibit it. Such Healthcare Facility policies that would be in effect shall be disclosed to NABIDH during the on-boarding process.

12.3.3.8. Mandatorily capture subject of care address including the Emirate ID, name, and categorize subject of care if they are Tourists.

12.3.3.9. Disclose all new policies established by Healthcare Facility to NABIDH after they join NABIDH. If the policy is not acceptable to NABIDH, then NABIDH may suspend access the system.

12.3.3.10. Allow only physicians to force access to all Health Information by “breaking the glass”, which shall trigger notification and after-the-fact review.

12.3.3.11. Allow Emergency Disclosures of Health Information when treating a Subject of Care with an Emergency Condition or “Breaking the Glass”.

12.3.3.12. A Consent is NOT required for NABIDH to Disclose Health Information to a Practitioner, an Authorized User that is acting under the direction of a Practitioner and those individuals may Break-the-Glass when the following conditions are met:

a. The Practitioner determines in his or her reasonable judgment that the Health Information, which may be available through the NABIDH System will be material to emergency treatment.
b. Healthcare Facility shall ensure that Break-the-Glass Disclosures of Health Information via the NABIDH System do not occur after completion of the emergency treatment.

- NABIDH does not require Consent for the uploading of Health Information to the NABIDH platform.

12.3.3.13. Enforce access control, including verification of consent status, at the time of use and disclosure of Health Information by healthcare providers.

12.3.3.14. Enforce that the individuals who access Health Information shall be responsible for protecting that information or preventing dissemination of that information.

12.3.3.15. Sensitive Health Information that require special protection above and beyond that of generic Health Information shall be marked as such.

12.3.3.16. A Healthcare Professional who agrees to a restriction requested by a Subject of Care must convey such restriction to the NABIDH team.

12.3.3.17. Ensure access to Health Information through clinician portal is permitted provided that:

a. The portal user shall abide by all NABIDH policies.
b. Agreements with the portal user shall be executed either with NABIDH or with a Healthcare Facility that is already bound to these policies.

12.3.3.18. Healthcare Facility to request access to authorized users who will send or receive Health Information to the NABIDH at any time.

12.3.3.19. Obtain Consent Form from Subject of Care in paper or electronic form through an Affiliated healthcare provider of the Healthcare Facility provided that:

a. Such Affiliated healthcare provider is providing healthcare services to the Subject of Care at the Healthcare Facility.
b. Such Affiliated healthcare provider is providing healthcare services to the Subject of Care in his or her capacity as an employee or contractor of the Healthcare Facility.
c. Such Affiliated healthcare provider is delivering healthcare services to the Subject of Care in the course of a cross coverage or on-call arrangement with the Healthcare Facility or one of it`s Affiliated facilities.

12.3.3.20. Each Healthcare Facility shall ensure that Subject of Care have the option, through the use of paper or electronic form, to deny consent for all HealthCare Facilities in the NABIDH Platform to Access or receive the Subject of Care's information.

12.3.4. The Subject of Care or the Subject of Care Agent shall:

12.3.4.1. Provide their consent on sharing their newly generated or past Health Information via NABIDH to HealthCare Facilities.

12.3.4.2. Confirm portal registration through access point (Ex: Mobile, e-mail etc.).

12.3.4.3. Be recorded in the NABIDH, when a Subject of Care chooses to Opt Out or opt in for sharing of Health Information.

12.3.4.4. Be aware that in the case where the Subject of Care has Opted Out of the NABIDH platforms, all relevant information will continue to flow into NABIDH platforms anonymously and may be used for research or public health purposes as per NABIDH Primary and Secondary use policy.

12.3.4.5. Be entitled to revoke a Consent at any time. Any Healthcare Facility that has accessed or received Health Information via the NABIDH Platform prior to such revocation and incorporated such PHI into its records may retain such information in its records.

13. SECTION 3: Incident Management and Breach Notification policy

13.1. Purpose:

15.1.1. To ensure appropriate tools, processes and procedures are in place to detect report and manage incidents and breach of protected PHI within the NABIDH Platform and for participating organizations.

15.1.2. To establish roles and responsibilities for individuals and HealthCare Facilities that have access to NABIDH managed PHI in order to prevent such breach within the NABIDH Platform.

13.2. Scope/ Applicability:

13.2.1. The scope of this document is the implementation of breach management for the NABIDH platform among DHA licensed healthcare providers in the Emirate of Dubai.

13.2.2. This policy applies to NABIDH, and to all individuals and Healthcare facilities that have access to NABIDH managed PHI, including:

13.2.3. DHA and their Business Associates or any subcontractors, who is responsible for oversight of NABIDH platform.

13.2.4. Public Health and their Business Associates or any subcontractors who is responsible for exchange of PHI.

13.2.5. NABIDH and their Business Associates or any subcontractors who is responsible for exchange of PHI.

13.2.6. Healthcare Facilities or Their Business Associates or any subcontractors who is responsible for submission, collection and use of PHI.

13.2.7. Subject of Care or the Subject of Care Agent who is responsible for providing appropriate consent to their PHI.

13.3. Policy statement:

13.3.1. Dubai Health Authority shall:

13.3.1.1. Develop and oversee the implementation of policies, standards, and guidelines related to the protection of PHI and specify the requirement for identification, notification and management of incidents and breach of information managed by NABIDH in accordance with all applicable UAE laws and DHA regulations.

13.3.1.2. Be held responsible for unauthorized disclosure of information accessed via the NABIDH Platform by their staff.

13.3.1.3. Enforce continuous improvements related to regulatory and compliance frameworks.

13.3.2. NABIDH shall:

13.3.2.1. Establish processes and responsibilities for management of incidents in compliance with the Health Information Security Standards to protect and prevent breach of Health Information within the NABIDH Platform.

13.3.2.2. Implement appropriate technical and organizational measures to protect against accidental, negligent or unlawful loss, disclosure or access to PHI, particularly in the context of processing or transfer of PHI to recipients.

13.3.2.3. Ensure all Healthcare Facility and individual users are made aware of their responsibilities for reporting information security incidents/ events/weaknesses, including whom to report and the location of the applicable policies/procedures.

13.3.2.4. Perform vulnerability assessments of the security measure of NABIDH to determine where weaknesses may exist and improvements can be made.

13.3.2.5. Notify vendors and/or certifying bodies of failures in system security controls.

13.3.2.6. Notify all affected parties and stakeholders of the security incident and possible consequences e.g. loss of data integrity.

13.3.2.7. Establish and publish a process for incident logging, response, handling, escalation and recovery to inform and guide those required or eligible to file reportable events and incidents. This process will take into account the privacy of information of Subject of Care involved in the reportable events and incidents.

13.3.2.8. Establish a common point of reporting for significant information security incidents to Nabidh@dha.gov.ae

13.3.2.9. Appoint the NABIDH Information Security Officer with defined roles and responsibilities for management of incidents.

13.3.2.10. Ensure NABIDH Information Security Officer audits and monitors the incidents of breach on a regular basis within NABIDH and HealthCare Facility.

13.3.2.11. Develop quarterly summary report of all reported events and incidents within the NABIDH platform.

13.3.2.12. Ensure NABIDH Information Security Officer contacts NABIDH users and Healthcare Facility that have access to the NABIDH, to review any suspicious activity. In case of an incident or reportable event, NABIDH Information Security Officer and Healthcare Facility Information Security Officer shall immediately investigate the suspicious activity and generate a report of the event.

13.3.2.13. Notify the concerned Healthcare Facility Information security officer(s) or designee and the Subject of Care in the event that a breach is identified and investigated by the NABIDH Information Security Officer.

13.3.2.14. Ensure NABIDH Information Security Officer receiving the Incident report or reportable event Report shall log the incident or reportable event.

13.3.2.15. The NABIDH Information Security Officer shall acknowledge the receipt of the Reportable Event Report to the person or system, filing it within 48 hours or two (2) business working days, and inform the affected Healthcare Facility Information Security Officer or designee of the event, if they do not already have knowledge of it, and subsequently begin a review of the event.

13.3.2.16. Ensure that, upon receipt of a reportable event or incident, it shall be reviewed by the NABIDH Information Security Officer to determine whether an investigation is required.

13.3.2.17. Facilitate protection of PHI, collection of evidence related to the reported incident and identity involving staff disciplinary or legal action.

13.3.2.18. Identify the need to revoke Healthcare Facility and/or individual users' accesses to NABIDH and as a result of the reported incident, develop measures to handle duress situations on a case to case basis.

13.3.2.19. Ensure that all relevant incidents and reportable events shall be investigated based on the incident priority matrix to identify the root cause within a maximum of 30 days and submit a final written report to the concerned parties (Appendix 4).

13.3.2.20. Determine that no further action is needed; this shall be communicated to the originator of the incident or reportable event, thus terminating the review process. Such decisions are subject to review through internal or external audits, based on the organizational framework of NABIDH.

13.3.2.21. Ensure that time and scope constraints for the investigation on the incident or reportable event of a confirmed breach will be a maximum of thirty (30) days, followed by mitigation actions taken within 180 days.

13.3.2.22. Ensure that in the case of an imminent threat to data security within NABIDH, the NABIDH Information Security Officer shall take immediate actions to secure the data, which could lead

to suspension of individual and Healthcare Facility user(s) access or account revocation.

13.3.2.23. Suspension of access privileges and/or account revocation may be enforced until the source of incident has been mitigated locally or possibly permanently as considered on a case-by-case basis.

13.3.2.24. Healthcare Facility shall fully cooperate with the NABIDH Information Security Officer in identification and mitigation of the threat that could result in a breach event.

13.3.2.25. Once the review is done, the NABIDH Information Security Officer shall determine whether a violation of privacy and security policies, procedures, or relevant law has occurred.

13.3.2.26. Notify DHA of any breach as soon as reasonably practicable after determining that a breach occurred, but in any event within 48 hours.

13.3.2.27. An incident Investigation Report shall be prepared, documenting the facts gathered from the review, event mitigations, and measures to be taken to prevent recurrence of such an event.

a. The Investigation Report shall be completed within thirty (30) calendar days of receiving the reportable event Report by NABIDH.
b. This timeframe MAY be extended for another 30 days on a case by case basis. This extension in the Breach Investigation Report shall be communicated to the originator of the Reportable Event Report or incident.

c. This report shall be retained for a minimum of twenty five (25) years, in compliance with DHA guidelines for managing health records.

13.3.2.28. When a Reportable Event is established as a privacy breach, NABIDH shall notify the HealthCare Facility, whose information was subject to unauthorized acquisition, access, use, or disclosure, no later than 48 hours or 2 business working days following the discovery of the breach.

13.3.2.29. When a breach occurs at the HealthCare Facility, any required public notification is the responsibility of the HealthCare Facility. If a breach occurs at NABIDH level, then, it's the responsibility of NABIDH to report the breach. In some situations, (e.g. where it is determined that it is important for the communication to be initiated by the healthcare provider organization rather than NABIDH), NABIDH shall to report to the HealthCare Facility, which shall in turn make any required public notifications. Such notification shall be made within thirty (30) days following discovery of the breach.

13.3.2.30. Ensure the notification to the Subject(s) of care shall contain, to the extent possible, the following:

a. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
b. A description of the types of PHI that were involved in the breach (such as full name, national identification number, date of birth, home address, etc.). The steps individuals should

take to protect themselves from potential harm resulting from the breach.

c. A brief description of what Healthcare Facility and NABIDH are doing to further investigate the breach, to mitigate harm to individuals, and to protect against any further breaches.

d. Contact procedures for individuals to ask questions or learn additional information, which shall include a telephone number, an email address, a web site, or postal address.

e. Procedure to report a petition with DHA in case the subject(s) of care are unhappy with the results of the investigation and corresponding actions.

13.3.2.31. Ensure breaches involving a single Individual and breaches involving small numbers of individuals should be reported to the Subject of Care involved in the breach. Breaches affecting large numbers of individuals, typically more than five hundred and involving continuous risk should be reported to DHA. The NABIDH Information Security Officer shall make such decision in collaboration with NABIDH and DHA.

13.3.2.32. Ensure NABIDH Information Security Officer and the Healthcare Facility Information Security Officer(s) involved in the incident shall collaborate to develop, approve, and implement the mitigation plan to proactively prevent a similar breach from re-occurring.

13.3.2.33. Ensure that the NABIDH Information Security Officer shall review existing policy for necessary changes to avoid any further breaches.

13.3.2.34. Ensure that the NABIDH Information Security Officer shall conduct the required educational campaign within NABIDH and associated organizations as necessary to educate employees on how to avoid further breaches.

13.3.2.35. Ensure that the NABIDH Information Security Officer shall take appropriate disciplinary action regarding the individual responsible for the breach, in accordance with the Information Technology Law (ICT) Law (article 25).

13.3.2.36. NABIDH Privacy & Security officer has to report the information security incidents to the DHA Information Security Office.

13.3.3. <u>All Healthcare Facilities shall:</u>

13.3.3.1. Oblige to follow the NABIDH breach notification policy for all incidents and reportable events involving the breach of protected PHI within the NABIDH Platform.

13.3.3.2. Develop and implement internal policies and procedures regarding beaches, which describe the different mechanisms for reacting to such breaches based on the priority of incidents (Appendix 4), and must include an internal notification process and a root cause analysis.

13.3.3.3. Update and provide periodic trainings for Authorized Users within the Healthcare Facility regarding identifying and notifying breaches within the NABIDH platform.

13.3.3.4. Be held responsible for unauthorized disclosure of information accessed via the NABIDH Platform by their staff.

13.3.3.5. Allocate an Information Security Officer(s) or appropriate designee to audit and monitor the security measures and review any suspicious activity on a monthly basis.

13.3.3.6. Ensure the Healthcare Facility Information Security Officer(s) or designee shall fully cooperate with the NABIDH Information Security Officer in identification, investigation, assessment and mitigation of reportable events involving their Healthcare Facility and/or Subject of care.

13.3.3.7. Ensure the Healthcare Facility Information Security Officer(s) or designated person shall communicate all incidents and reportable event and reviews to the concerned authorities in NABIDH, within (48 hours) of the discovery of an incident in accordance with the Breach Notification Policy.

13.3.3.8. Notify subject of cares affected, and any applicable regulatory agencies as required in accordance with Applicable Laws.

13.3.3.9. Ensure the Healthcare Facility Information Security Officer(s) or designee shall conduct internal review of the incidents and also cooperate with the NABIDH Information Security Officer in investigation, assessment and mitigation of reportable events involving their Healthcare Facility and/or Subject of care.

13.3.3.10. Ensure that the Healthcare Facility Information Security Officer is responsible for preventing further breaches and incidents within the Healthcare Facility.

13.3.3.11. Ensure that the Healthcare Facility Information Security Officer shall review existing policy for necessary changes to avoid any further breaches.

13.3.4. The Subject of Care or the Subject of Care Agent shall:

13.3.4.1. Ensure in the case of a suspected breach, identified by the Subject of Care, he or she can initiate a notification of incident or reportable events using the complaint form or other means, which shall be accepted by the Healthcare Facility Information Security Officer and further can request an investigation as per the Breach Notification Policy. This incident shall be reported to the NABIDH Information Security Officer.

13.3.4.2. Direct the request to the NABIDH Information Security Officer, if the results of investigation from the Healthcare Facility is considered unsatisfactory by the complainant.

14. SECTION 4: Audit Policy

14.1. Purpose:

14.1.1. To define compliance and audit requirements for the NABIDH Platform.

14.1.2. To assure effectiveness of implemented information security controls and prevent violations and breaches as per the laws, policies, or controls within the UAE.

14.1.3. To provide guidance in identifying and preventing unauthorized access to PHI within the NABIDH system and to comply with relevant privacy requirements.

14.1.4. To define the roles and responsibilities of all the relevant participants within the NABIDH system

14.1.5. To have an effective auditing process that ensures confidentiality of PHI within NABIDH.

14.1.6. To define the frequency and specifications of maintaining Audit Logs for maintaining Audit Logs for documenting all the access to and receipt of PHI through the NABIDH system.

14.2. Scope/ Applicability:

14.2.1. The scope of this document is the specification for audit requirements for implementation of the NABIDH platform among DHA licensed healthcare providers in the Emirate of Dubai.

14.2.2. This policy applies to NABIDH, and to all individuals and Healthcare facilities that have access to NABIDH managed PHI, including:

14.2.3. DHA and their Business Associates or any subcontractors, who is responsible for oversight of NABIDH platform.

14.2.4. Public Health and their Business Associates or any subcontractors who is responsible for exchange of PHI.

14.2.5. NABIDH and their Business Associates or any subcontractors who is responsible for exchange of PHI.

14.2.6. HealthCare Facilities, their Business Associates or any subcontractors who is responsible for submission, collection and use of PHI.

14.3. Policy Statement:

14.3.1. Dubai Health Authority Shall:

14.3.1.1. Develop and implement standards and guidelines on auditing the performance and security features of the NABIDH platform in accordance with all relevant legislative statutory, regulatory, and contractual requirements.

14.3.1.2. Continuously improve the related regulatory and compliance frameworks.

14.3.1.3. Perform annual audits on the NABIDH platform and their appointed third-party vendor to ensure compliance with all applicable Laws and Policies.

14.3.2. NABIDH shall:

14.3.2.1. Implement technical processes that accurately record all activities related to access, creation, modification, disclosure and deletion of electronic PHI that facilitates the auditing process of the NABIDH Platform as per the NABIDH Audit Policy and standards.

14.3.2.2. Assure all HEALTHCARE FACILITY node and NABIDH systems shall be configured to generate logs of all events (e.g. login, logoff, access events, denial events, etc.) as supported by installed products to enable further investigation and traceability.

14.3.2.3. Audit the compliance with applicable legislative, regulatory and contractual requirements related to intellectual property rights and use of copyrighted/licensed materials, software or applications.

14.3.2.4. Perform regular audit on the compliance of information processing and procedures relating to the security policies, standards and any other security requirements.

14.3.2.5. Perform a risk assessment for all information systems periodically, or following significant business or technology changes to systems, contract renewals, extensions and/or vendor changes.

14.3.2.6. Undertake an independent review of the Healthcare Facility approach to managing information security and its implementation (i.e., control objectives, controls, policies, processes and procedures for information security) at planned intervals or when significant changes occur.

14.3.2.7. Conduct reviews and reports on NABIDH information assets assurance processes regarding security matters (e.g., incidents,

responses, issues, risks). This may include undertaking specialist internal/external audits of their environments and taking appropriate action based on findings and recommendations.

14.3.2.8. Establish defined responsibilities to the Health Informatics and Smart Health Department (HISH) for periodically auditing of the performance and compliance for the NABIDH platform. Health Informatics and Smart Health Department (HISH) shall be responsible for recommending the frequency of the audits to be performed, the specific controls to be audited and notifying participants and determining the sample size for each audit. The department shall also review the results of the audits and any corrective action to be taken as a result of problems uncovered during the audits and make recommendations as to whether the specified corrective action should be accepted.

14.3.2.9. Define the audit log to include specific audit functions including but not limited to:

a. Review of system administrator authorizations and activity.
b. Review of network intrusion detection system activity logs.
c. Review of physical access to data centres.
d. Procedures for follow-up on suspicious activity, such as indications of possible privacy or security breaches.
e. Other review of technical, physical, and administrative safeguards as established by the policies of the organization

14.3.2.10. Ensure audit logs are either in human readable format or translatable by some easy to use tool to be in human readable format.

14.3.2.11. Ensure audit logs are retained for Three (3) years, the same duration as the retention time required of NABIDH managed PHI.

14.3.2.12. Ensure audit log review of the systems shall include but not limited to software applications, networks, servers, firewalls and other network hardware and software:

a. All system logs shall be reviewed by the nominated designee from the respective HealthCare Facility.

b. The generated audit logs shall be reviewed on a regular basis based on audit criteria developed in advance, at least quarterly, in order to detect improper use of the PHI.

c. All anomalies shall be documented and appropriate mitigating action shall be taken and documented.

d. All system audit logs and evidence shall be provided to Health Informatics and Smart Health Department (HISHD) upon request for any investigation.

14.3.2.13. Ensure privacy and security audit review shall support inquiry by stakeholders and users.

14.3.2.14. Ensure external audits of the NABIDH shall be conducted at least annually as a minimum requirement and when any major system or business change occurs. Comprehensive audit procedures

should be developed, documented, and made available. The external audit shall include:

a. The generation of a compliance audit findings report and documentation of any identified deficiency that needs to be addressed in order of priority.

14.3.2.15. Ensure audit record repository system includes the following but not limited to:

a. List all users that accessed or modified a given Subject of Care's information over a period of time.
b. List all Subjects of Care whose Health Information was accessed by a given user/system over a given period of time,
c. List of all break glass events,
d. List all access events where the user is not listed as a provider in any subject of care records, and
e. List events that request information marked as sensitive.

14.3.2.16. A valid date, time, and stamp shall be used for data authentication purposes.

a. All HIE nodes exchanging PHI shall implement the time synchronization mechanism specified by NABIDH to assure that timestamps and audit logs are synchronized.

14.3.2.17. Ensure that the audit logs repository is secured in accordance with the NABIDH information security standard (Section 8). Access to system audit log analysing tools and audit logs shall be safeguarded to prevent misuse or compromise.

14.3.2.18. Ensure that NABIDH audit logs access are restricted only to the respective designated assignees from Healthcare Facility and NABIDH.

14.3.3. <u>All Healthcare Facilities shall:</u>

14.3.3.1. Implement technical processes and policies for accurate, timely, and secure recording of activities related to access, creation, modification, disclosure, and deletion of electronic PHI that facilitates the auditing process in compliance with the NABIDH Platform and this policy.

14.3.3.2. Successfully complete all required audit testing for all applications by NABIDH users. Applications that have not yet completed this testing will be considered on a case-by-case basis.

14.3.3.3. Log all transactions of clinical data within the NABIDH Platform to support periodic auditing and to have all activities logged locally, and maintained in a persistent database.

14.3.3.4. Ensure that log files are not altered, in order to prevent sophisticated attackers from removing traces of their work. Such logs must not contain the full record being transmitted, so that the logs themselves do not become an alternate target for attackers looking for clinical information.

14.3.3.5. Ensure that, as part of log-in monitoring, an audit log shall be created and maintained to record user logs on to the NABIDH platform. This should include all attempted and failed logons.

14.3.3.6. Ensure that for the purposes of information use or disclosure, the audit log shall include the following documentation of the request to access to the PHI through the NABIDH platform:

a. The date and time of the request.
b. Location of access.
c. The reason for the request.
d. A description of the information requested, including the data accessed, the data transmission, any changes to the data (adds, changes, deletes), and whether the data were transmitted to another party.
e. Whether the request was performed as a “break glass”.
f. Whether the requested information was marked as sensitive PHI.
g. Whether the access is made by a privileged account user.
h. The ID of person/system requesting the access to PHI.
i. The ID of the person/system generating response for PHI access requests.

14.3.3.7. Be responsible to recommended corrective actions to NABIDH in response to problems uncovered during the audits and implement the approved corrective actions and along with additional corrective actions recommended by the NABIDH privacy and security committee as a result of audit reviews.

14.3.3.8. Have the ability to generate an electronic access report summary of PHI exchanged for all applications within the NABIDH.

a. This capability shall be demonstrated when integrating the Healthcare Facility Node to the NABIDH system
b. Testing of this capability shall be conducted by NABIDH.
c. The Healthcare Facility should be able to audit all access to PHI that is stored locally.

15. SECTION 5: Data Management and Quality Policy (Primary and Secondary Use)

15.1. Purpose:

15.1.1. To define permissible uses of the NABIDH data such as Primary Use (Subject of care Care) and Secondary use (Research, Public Health, Quality Improvement and Safety Initiatives.).

15.1.2. To ensure data is used and accessed only as permitted by applicable UAE Laws and DHA regulations.

15.2. Scope/Applicability:

This policy applies to everyone involved in the protection of PHI including:

15.2.1. Dubai health authority and their Business Associates or any subcontractors, who is responsible for oversight of NABIDH platform.

a. Dubai health authority Public Health and their Business Associates or any subcontractors who is responsible for exchange of PHI.
b. NABIDH and their Business Associates or any subcontractors who is responsible for exchange of PHI.
c. Healthcare Facilities or Their Business Associates or any subcontractors who is responsible for submission, collection and use of PHI.

d. Subject of Care or the Subject of Care Agent who is responsible for providing appropriate consent to their data.
e. All parties requesting to use the NABIDH managed information for secondary use.

15.3. General Use and Disclosure:

Primary use of PHI is defined as exclusive use by the organization that acquired the data, in providing direct care to the subject of care. Secondary uses are those that are used for health system planning, management, quality control, public health monitoring, program evaluation, and research. Some secondary uses directly complement the needs of primary use. Examples include medical billing, hospital administrative, and management operations. While some secondary use includes usage that support medical research and public health, organization sales, marketing, and financial gain. Secondary use regularly occurs without the subject of care's knowledge or consent.

15.4. Compliance with Law

All disclosures of PHI through the NABIDH and the use of information obtained from the NABIDH shall be consistent with all applicable UAE ICT laws and DHA regulations and shall not be used for any unlawful discriminatory purpose.

If the UAE ICT law requires that certain documentation exist or that other conditions be met prior to using or disclosing PHI for a particular purpose, the requesting Participant shall ensure that, it has obtained the required

documentation or met the requisite conditions and shall provide evidence of such at the request of the disclosing Participant.

15.5. Policy Statement:

Personal Health Information will primarily be made available in NABIDH for purposes of Treatment, Healthcare Operations, Public Health and research:

15.5.1. Primary Use:

15.5.1.1 Clinical Care Provision to an Individual Subject of Care

The information collected by the healthcare provider for the primary purposes of giving treatment and health care to the subject of caret.

15.5.1.2 Emergency Care Provision to an Individual Subject of Care.

To inform individuals needing to provide healthcare services to the Subject of Care urgently and possibly needing to override the NABIDH consent policy pertaining to clinical care provision.

To inform individuals or processes enabling others (e.g. healthcare providers who have a legitimate right to provide care) to provide healthcare services to the Subject of Care.

15.5.1.3 Subject of Care Uses

To inform the Subject of Care in support of his or her own interests. Subject of Care identification upon presentation for medical treatment.

a. Subject of Care diagnosis, treatment, and related Healthcare Operations, etc.
b. Share Health Information data received from outside or inside the United Arab Emirates and access it through the NABIDH Platform.
c. Subject of care to share PHI data if required to healthcare facilities outside UAE in order to facilitate their treatment abroad as per Article 13 of ICT law 2019.

15.5.2. Secondary Use:

Personal Health Information on the NABIDH may be made available for the following purposes other than Treatment or Operations directly related to subject of care healthcare. For the purpose of Health Service Management and Quality Assurance:

15.5.2.1 Risk management, error management or for the purpose of activities to improve or maintain the quality of care or to improve or maintain the quality of any related programs or services

15.5.2.2 To inform healthcare facilities and regulatory bodies in DHA on determining the availability, quality, safety, equity and cost-effectiveness of healthcare services.

15.5.2.3 Data or Health Information required by the health insurance companies or any provider of health services in respect of the health services received by the subject of care for purposes of auditing,

approving or verifying the financial benefits related to those services.

15.5.2.4 All Individual Health Information in the NABIDH will be available for public health and quality reporting. The NABIDH consent policy permits covered entities to disclose protected Health Information, without authorization, to public health authorities who are legally authorized to receive such reports for the purpose of preventing or controlling disease, injury, or disability. This would include, for example, the reporting vital events, such as births or deaths; and conducting public health surveillance, or quality investigations.

15.5.2.5 Public Health Surveillance, Disease Control:

a. To inform individuals or processes with responsibility to monitor populations or sub- populations for significant health events for Purpose of preventive and curative measures related to public health, or to maintain the health and safety of the subject of cares or any other persons in contact with them.

b. Public Safety Emergency.

c. To inform individuals with responsibility for the protection of the public in a situation in which there is considered to be a significant risk to one or more members of the public Population Health Management.

d. To inform individuals or processes with responsibility to monitor populations or sub- populations for health events,

trends or outcomes in order to inform relevant strategy and policy.

15.5.2.6 To support Education, learning and professional development.

15.5.2.7 At the request of the competent judicial authorities.

15.5.2.8 At the request of the health authority for the purposes of inspection, supervision and protection of public health.

15.5.2.9 Organ Transplant:

a. Grant UAE Organ Procurement Organization access to the NABIDH solely for the purpose of facilitating organ, eye or tissue donation and transplantation as per federal law no 5 for year 2016 and legislation no 25 for year 2020.

15.5.2.10 Research:

a. For the purposes of scientific and clinical research, provided that the subject of care's identity is not disclosed and that the ethics and rules of scientific research are followed as per ICH_GCP principles and guidelines.

b. To support the discovery of scientific facts that will add into generalizable knowledge.

c. Any data sets need to be approved by Dubai Scientific Research Ethics Committee (DSREC) and must follow the principle of least privilege use.

d. Dubai Scientific Research Ethics Committee approval shall be considered on a case-by-case basis.

e. Any additional approval requirements and other proposal criteria requesting access to such data shall be determined and published by the DSREC.

f. The Dubai Scientific Research Ethics Committee may publish criteria (e.g., may have a minimum necessary content for the proposal) that the principal investigator shall follow.

g. The NABIDH Privacy and Security Officer or designee shall be informed about the DSREC outcomes related to NABIDH Health Information data use by DSREC chairperson in written.

h. This notification from DSREC should include type of data to be extracted from NABIDH, name of the principal investigator (PI), name of the facility the PI is working in, and timeframe of data to be extracted by the PI.

i. Research data extracts or views shall be facilitated by the NABIDH approved subcontractor.

j. A Data Use Agreement for Health Information between the research organization/individual and the NABIDH shall be established.

k. The Data Use Agreement shall include the following requirements:

    (i) The data use and access shall be limited to the specified purpose cited in the approved research proposal.

    (ii) Additional authorizations and consents of study

subjects may be required in some scenarios, as defined by the DSREC. Where authorizations and consents are required, the NABIDH shall have access to the authorizations and consents.

(iii) The DSREC may require that the data be de-identified without re-identification capabilities.

(iv) In the case where a view is provided to the data set that would be managed by the NABIDH, the party requesting the data shall identify designated individuals that access the data for the approved purpose.

15.5.2.11 De-identified Health Information may be released from the NABIDH under the following conditions:

a. De-identification methods shall undergo a re-identification risk assessment of the proposed data extract.

b. The DSREC may consider the request on a case-by-case basis.

c. The DSREC may offer criteria that will allow documentation of de-identified data sets that are not subject to case-level consideration and approval (e.g. re- identification risk criteria of routine de-identified information sets)

d. Research record should be retained for at least ten (10) years after the release of the information.

15.5.3. Uses that shall not be Permitted:

Following are some of the examples of non-permitted uses of Subject Of care data received via the NABIDH Platform but are not limited to:

15.5.3.1 Exploiting Health Information for the purposes of unlawful gains, whether personal or otherwise.

15.5.3.2 A Healthcare Professional disclosing Health Information that became known to him/her in the course of or due to the practicing of his or her profession, otherwise than as may be allowed in the Policies or Applicable Law.

15.5.3.3 Access or use of personally identifiable PHI by Healthcare Professionals who are not associated with the treatment of that specific Subject of care or cohort of Subject of cares.

15.5.3.4 Distribution to Third Parties.

15.5.3.5 Granting access to Third Parties.

15.5.3.6 Use for commercial gain or marketing purposes.

15.5.3.7 Use of Health Information to form a Health Information exchange (other than the NABIDH Operator).

15.5.3.8 Sub-licensing of Health Information.

15.5.3.9 Storage of Health Information in a cloud environment.

15.5.3.10 Ingesting, storing, or recording any Health Information that is received or made available from or accessed through the NABIDH Platform into its own system.

16. SECTION 6: Identity Management Policy

16.1. Purpose:

16.1.1. To define the identity management requirements for a secure system level access and to ensure systems and individuals interacting with NABIDH are known through a process of reliable security identification by incorporating identifiers and its authenticators.

16.1.2. To establish the categories of users and their respective identity authentication parameters within the NABIDH platform.

16.2. Scope/ Applicability

16.2.1. The scope of this document is the specification for audit requirements for implementation of the NABIDH platform among DHA licensed healthcare providers in the Emirate of Dubai.

16.2.2. This policy applies to NABIDH, and to all individuals and Healthcare facilities that have access to NABIDH managed Health Information, including:

16.2.2.1 DHA and their Business Associates or any subcontractors, who is responsible for oversight of NABIDH platform.

16.2.2.2 Public Health and their Business Associates or any subcontractors who is responsible for exchange of PHI.

16.2.2.3 NABIDH and their Business Associates or any subcontractors who is responsible for exchange of PHI.

16.2.2.4 HealthCare Facilities, their Business Associates, or any subcontractors who is responsible for submission, collection and use of PHI.

16.2.2.5 Subject of Care or the Subject of Care Agent who is responsible for providing appropriate consent to their data.

16.3. Policy Statement

16.3.1. Dubai Health Authority shall:

16.3.1.1 Develop and implement standards and guidance on identity authentication and management for users of the NABIDH platform in accordance with all applicable Laws and DHA Regulations.

16.3.1.2 Continuously improve related regulatory and compliance frameworks.

16.3.2. NABIDH shall:

16.3.2.1 Define specifications that qualify as National Identifiers to authenticate the various categories of users for the NABIDH platform

16.3.2.2 Assume full authority for granting access privileges to users, based on the authentication of identities by Healthcare Facility for each of its approved users.

16.3.2.3 Identify entities for verification and management of digital certificates for NABIDH users from Healthcare Facility and their Business Associate.

16.3.2.4 Ensure that the identity of individual users accessing the NABIDH system shall be subject to identity verification for the issuance of access credentials.

16.3.2.5 Ensure that federated identity proofs be applied to authenticate users to the NABIDH platform on a case by case basis.

16.3.2.6 Define the requirements for Proof of Identity for individuals as follows:

a. Identity Proofing for all individual users shall include a face-to-face verification of the individual's identity.

b. Identity proofing for all individual users shall require a valid government issued photographic identification. The National Emirates ID shall be the primary identification document; however, passport, driver's license, DHA employee ID or Residency Permit for Residents or a government recognized biometric identification can be considered in absence of the National Emirates ID.

c. For Subject of Care, the identity proofing will be conducted at the Healthcare Facility with a valid government issued photographic identification. The primary identification document shall be the updated National Emirates ID. However, valid passport, driver's license or Residency

Permit for Residents or other government recognized biometric identification shall be accepted in the absence of the National Emirates ID. The Emirates National ID shall be duly updated as per validity in the NABIDH platform. Antecedent Data (e.g. from a prior health visit) may be used as the face-to-face verification of the individual's identity.

d. For Subject of Care agent, additional proofing shall be provided indicating authorization to act on behalf of the Subject of Care for access to NABIDH.

e. Identity Proofing for Regulated Health Professional requires evidence of a current healthcare license issued by the Dubai Health Authority in addition to the Identity Proofing requirements that apply to all individuals.

f. Identity Proofing for Non-Regulated Health Professionals shall require verification of employee ID or letter from employer on employer letterhead indicating current employment status in addition to the Identity Proofing requirements that apply to all individuals.

g. Identity Proofing of a Sponsored Healthcare Provider shall require a letter from a Regulated Healthcare professional or authorized

h. Representative of a sponsoring regulated health organization to establish that they are active in their healthcare community OR evidence of current credentials

issued by the Dubai Health Authority in addition to the Identity Proofing requirements that apply to all individuals.

i. For other users (e.g. researchers), antecedent data may be used to provide limited access to NABIDH platform.

j. Be informed on Healthcare or non-healthcare professionals who are terminated from Healthcare Facility and determine the termination of access to those users on case-to-case basis. An acknowledgment of receipt of notification on employee termination should be issued upon receipt.

16.3.2.7 Be informed by the Healthcare Facility upon individual user's role modification for any employee who has been issued an individual identity credential to access NABIDH. An acknowledgment of receipt of notification on employee role modification should be issued upon receipt.

16.3.2.8 Establish defined requirements for Proof of Identity for Healthcare Facility and Organization's systems as follows:

a. Verification by an individual identified by the organization as authorized to provide such attestation.

b. A letter on the entity letterhead signed by a corporate officer shall identify the representative of the entity, authorized to validate and request organization or device certificates on behalf of the entity that will be used for the provision of Healthcare Facility certificates.

c. The Organization responsible shall provide proof of a current license to conduct the healthcare or healthcare associated

business, a valid commercial registration document by a nationally recognized government entity.

16.3.2.9 Ensure Healthcare Facility agreements include the requirement to protect their identity credential.

16.3.2.10 Establish a process for Healthcare Facility to notify the NABIDH Privacy and Security officer, if their digital identity is lost, stolen, or otherwise known to be compromised. Further, on, a revocation request shall be launched along with a request for a new digital identity. Refer to NABIDH Breach Notification Policy for reporting.

16.3.2.11 Maintain a log-list of all individuals and Healthcare Facility along with their respective identity authentication documents that have access to the NABIDH system along with the data contribution endpoint infrastructure. The list must include the following:

a. The ID credentials.
b. Person or information system's details: full name, department, and location, and contact information (email and telephone number, where available)
c. Identity proofing documents

16.3.3. <u>All HealthCare Facilities shall:</u>

16.3.3.1 Implement initial identity-proofing procedures, in accordance with the Identity Management Policy, that requires Authorized Users to provide identifying materials

and information upon application for access to the NABIDH Platform.

16.3.3.2 Be responsible for authenticating each individual authorized User's identity prior to granting access to NABIDH Platform.

16.3.3.3 Assign a unique name and/or number to all Authorized Users within the healthcare facility that access the NABIDH Platform for identifying and tracking user identity.

16.3.3.4 Be subject to verification by NABIDH for the issuance of identity credentials.

16.3.3.5 Be subject to verification by NABIDH for utilization of digital certificates.

16.3.3.6 Be responsible for identity proofing for all Subject of Care. The identity proofing will be conducted at the Healthcare Facility with a valid government issued photographic identification.

16.3.3.7 For Subject of Care agent, additional proofing shall be provided indicating authorization to act on behalf of the Subject of Care for access to NABIDH platform.

16.3.3.8 Ensure procedures for account revocation upon employee termination are implemented:

a. Notification to NABIDH shall be issued at least two days prior to the last date of service termination.

b. Receive an acknowledgment of notification from NABIDH.

c. Account revocation by the Healthcare Facility and NABIDH should be set in the NABIDH platform to ensure access revocation within two business days after receiving notification.

16.3.3.9 Ensure procedures for account revocation upon employee severance due to misuse of PHI data are implemented in alignment with the NABIDH Breach Notification Policy (Section 3).

a. Notification to Sheryan and NABIDH shall be issued with immediate effect for healthcare professionals.

b. Notification to NABIDH shall be issued on immediate effect for non-healthcare professionals.

c. Receive and acknowledgment of receipt of notification.

d. Account revocation by the Healthcare Facility and NABIDH should be implemented with immediate effect after the receipt of notification.

16.3.3.10 Ensure procedures for account update upon employee role modification for any employee who has been issued an individual identity credential to access NABIDH are implemented:

a. Notification to NABIDH should be issued within two business days.

b. Receive an acknowledgment of receipt of notification should be issued upon receipt.

c. Account update by the Healthcare Facility and NABIDH should be implemented within two business days after notification

16.3.3.11 Ensure to notify the NABIDH Privacy and Security officer, if their digital identity is lost, stolen, or otherwise known to be compromised. Refer to NABIDH Breach Notification Policy for reporting (Section 3).

16.3.4. The Subject of Care or the Subject of Care Agent shall:

16.3.4.1 Provide their identity proofing to HealthCare Facility, in accordance with NABIDH Identity Management Policy.

16.3.4.2 Be subject to all identity verification procedures implemented by NABIDH for the issuance of identity credentials.

17. SECTION 7: Authentication and Authorization policy

17.1. Purpose:

17.1.1. To allow only authorized users and certified applications to access information through NABIDH.

17.1.2. To limit exchange of information to minimum number of individuals necessary for accomplishing the intended purpose of the exchange.

17.1.3. To embed confidence in the privacy of subject of care Health Information as it is transferred across the health system to meet their needs.

17.2. Scope:

This policy applies to all users accessing and using NABIDH including:

17.2.1. DHA and their Business Associates or any subcontractors, who are responsible for oversight of NABIDH platform.

17.2.2. NABIDH and their Business Associates or any subcontractors who are responsible for exchange of subject of care Health Information.

17.2.3. HealthCare Facilities and their Business Associates or any subcontractors who are responsible for submission, collection and use of subject of care Health Information.

17.2.4. Subject of Care or the Subject of Care Agent who is responsible for providing appropriate consent to their data.

17.3. Policy Statement:

17.3.1. Dubai Health Authority Shall:

17.3.2.1 Oversee the implementation of further policies, standards, and guidelines related to NABIDH Authentication and Authorization as necessary in accordance with applicable Laws and DHA Regulations.

17.3.2. NABIDH Shall:

17.3.2.2 Maintain Authentication and Authorization standards and protocols that are compliant with Applicable Laws, DHA regulations and DHA Health Information Security Standard (HISS) that all member participants must adhere to.

17.3.2.3 Users shall be authenticated against identity access management system.

17.3.2.4 Verify the user identity, role, and affiliation at the time of logon to the system. If any of these has been revoked or has expired, access shall be denied.

17.3.2.5 Suspend user access if the approved users do not use their access for 90 days.

17.3.2.6 Provide access once authorization procedures have been indicated by the relevant Healthcare Facility as being completed and list of Authorized Users has been received.

17.3.2.7 Authorization of users shall be role based taking into account an individual's job function and information required to carry out their role.

17.3.2.8 Define and establish categories of Authorized Users and access levels that will ensure that an end user can access types of information only if they are permitted to do so.

17.3.2.9 Categorize and define in the Participation Agreement the types of Subject of care Health Information that each category of Authorized User may access and the purposes for which they may access it.

17.3.2.10 Ensure that NABIDH system remote access by individual users shall require secure authentication process.

17.3.2.11 Ensure that all HIE Nodes exchanging Personal Health Information shall implement a node authentication mechanism compliant with security standards (Section 8).

17.3.2.12 The user sessions of the HIE node should be automatically logged off after no more than 15 minutes of inactivity.

17.3.2.13 In the case of suspected breach or virus attack or incidents, NABIDH has the right to turn off access to the node to avoid any further breach or damage.

17.3.2.14 Support Emergency Access to all care providers accessing the NABIDH as a break-glass with audit and review of these actions, in accordance with the Audit Policy. Notification should be sent to the subject of care and to the Data Privacy and Security officer.

17.3.2.15 Maintain a Registry of Participants within the NABIDH that may include primary contact information of registered users, roles/privilege information, and identity attributes of providers, organizations, and systems.

17.3.2.16 Ensure NABIDH is capable of identifying all users who have accessed, or modified a given subject of care/person's record(s) over a given period of time.

17.3.2.17 Conduct periodic access reviews including applications, infrastructure, Data centre and third parties.

17.3.3. HealthCare Facilities Shall:

17.3.3.1 Comply with all current applicable laws and regulations such as UAE ICT Law, DHA regulations, Federal and Local Laws, etc. regarding Authentication and Authorization of users.

17.3.3.2 Ensure compliance of all systems and processes using NABIDH with the DHA HISS.

17.3.3.3 Prior to providing access to NABIDH platform, verify and authenticate the identity of their Authorized Users within the scope of this policy to access Data through NABIDH (Section 6).

17.3.3.4 Authenticate the identity of Authorized Users through physical and digital identity checks before granting access to

NABIDH. The NABIDH shall require unique identification of the individuals (Healthcare Facility identifiers, employees, care providers, subjects of care, subjects of care agents), systems (HIE node, HIE system, or the Application), and Organizations accessing the information in the NABIDH.

17.3.3.5 Ensure that the level of access granted is appropriate to the business purposes of Authorized Users.

17.3.3.6 Ensure that each authorized user shall complete training prior to activation of access to NABIDH and these authorized users shall undergo refresher training on annual basis.

17.3.3.7 Develop, maintain and implement relevant access control policies and procedures. Each Participant will be responsible for designating its authorized users and establishing their level of access based on their job function.

17.3.3.8 Immediately terminate the user-access privileges of permanent or temporary employee or third-party contractor who is a registered user of system and who has access to NABIDH upon termination of their employment with the organization.

17.3.3.9 Notify Sheryan and NABIDH when Healthcare professionals are terminated from Healthcare Facility for misuse of Personal Health Information.

17.3.3.10 Notify NABIDH when non-Healthcare professionals are terminated from Healthcare Facility for misuse of Health Information.

17.3.3.11 Assert secure authentication process for remote access to NABIDH clinician portal (from outside of the physical control of the organization).

17.3.4. Subject of Care Shall:

17.3.4.1 Follow authentication process to access subject of care portal.

17.3.4.2 Refrain from disclosing portal passwords to any other person.

17.3.4.3 Inform NABIDH administrator or Healthcare Facilities administrators if the subject of care portal account is hacked or compromised.

17.3.4.4 Be responsible and liable for all actions including information retrieval or communication performed on subject of care portal.

18. SECTION 8: Information Security Standards

18.1. Purpose

18.1.1. To provide advice about procedures and technical standards that need to be incorporated in an information security policy

18.1.2. To set out minimum requirements and desired goals at various levels of health care provider operational complexity and risk.

18.1.3. To maintain the information's confidentiality, integrity and availability.

18.1.4. To identify, assess, record, prioritize and manage threats concerning the confidentiality, integrity and availability of the Health Information related physical and logical assets.

Confidentiality:	**Access to PHI is limited to authorized users for approved purposes.**
Integrity:	Data and information are accurate, consistent, authentic and complete. It has been properly created and has not been tampered with, damaged or subject to accidental or unauthorized changes. Information integrity applies to all information, including paper as well as electronic documents.
Availability:	Authorized users' ability to access classified information for authorized purposes at the time they need to do so.

Table 2: Information Security Standards – Purpose

18.2. Scope

18.2.1. This standard is concerned with the security of PHI wherever it may exist.

18.2.2. This document assumes personal PHI will be shared – it does not say what information is to be shared or under what circumstances (e.g., where identifiable PHI is anonymized). Restrictions on information sharing apply to Personally Identifiable Information (PII); PHI that has

been anonymized is not necessarily subject to the same sharing restrictions.

18.2.3. All subject of care-identifiable health care information is classified as per the classification scheme identified by each health care provider as a minimum equivalence to 'Shared-Sensitive' category as per "Law No.26 of 2015 Regulating Data Dissemination and Exchange in the Emirate of Dubai" and given an equal level of protection unless otherwise classified.

18.3. Application

18.3.1. The development and application of specific security policies and procedures to support the organisation is the responsibility of the organisation's management. However, compliance with the HISS framework's Risk management section 18.4 is mandatory

18.3.2. This standard applies, but is not limited to the healthcare providers integrated with NABIDH.

18.4. Risk Management

Health care organisations must undertake the following three activities as a minimum to meet their responsibilities in managing Health Information. They must identify and treat risks associated with health and related information and information assets through a detailed study of business processes, in determining threats and vulnerabilities and accordingly apply the appropriate risk treatment plans and controls.

18.4.1. Risk Assessment Methodology & Planning

18.4.1.1 Develops a risk assessment methodology that aligns with the requirements of the entity's information security program /management system.

18.4.1.2 Determines a periodic plan for conducting the risk assessment

18.4.1.3 Identifies the criteria of acceptable risks as part of the risk assessment

18.4.1.4 Identifies the scope of the risk assessments involving key stakeholders, around their business processes & respective information assets that will be included in the assessment.

18.4.1.5 Identifies threats and vulnerabilities in line with risk assessment methodology.

18.4.1.6 Plans and implements a periodic awareness of the risk assessment program across the entity.

18.4.2. Risk Assessment

18.4.2.1 Conducts and maintains a detailed risk assessment in accordance with the approved risk assessment methodology.

18.4.2.2 Develop and apply policies and procedures to address each of the identified risks

18.4.2.3 Regularly monitor and report on the performance of the above policies/procedures. This includes reviewing each policy/ procedure for effectiveness and updating the policies/procedures as needed.

18.4.2.4 In summary, the provision of appropriate effective Health Information security:

a. Is a requirement of management.
b. Must be tailored to the individual requirements and exposures faced by each health care organisation. The HISS provides guidance, ideas and comment to support these tasks.
c. Analyses risks and prioritizes them based on the criticality, in order to set treatment plans and controls.
d. Determines and identifies the acceptable risks in accordance with the risk assessment methodology.
e. Documents the risk assessment results and must get it approved by health care provider's higher management or an Information Security Steering Committee established at par.

18.4.3. Risk Treatment and Mitigation

18.4.3.1 Selects the proper risk treatment plans (mitigate, avoid, transfer, etc.) For the identified risks.

18.4.3.2 Determines and selects the appropriate security operational controls (under operational domains within this document) for mitigating the identified risks.

18.4.3.3 Signs off and authorizes officially the implementation of the risk mitigations controls.

18.4.3.4 Performs and implements the mitigation controls for the risks identified.

18.4.3.5 Reviews and monitors the implemented risk mitigation controls for effectiveness.

18.3.1. Risk Acceptance

Documents the residual non treated risks with justifications and gets it signed off from the Information Security Steering Committee along with the detailed plan for treatment at a later date.

18.5. Organization and Control categories

HISHD directs the minimum areas of policy, and associated controls, to be developed and applied by all healthcare services providers before getting on-boarded to NABIDH HIE Platform.

The requirements for each individual security section have been grouped into three organisation compliance categories.

Organization Category	Category Indicator(s)
Essential	The controls outlined in the "**ESSENTIAL**" category are the **absolute minimum**. Compliance with this level is required of all health care (or support) organisations ready to be on boarded to NABIDH
Intermediary	Organisations are required to achieve "**INTERMEDIARY**" level for some or all categories. This is based on the type of data they hold, functions they perform or a heightened level of risk they are exposed to as per the reviewed Risk Assessment performed in line with controls described in section (5).
Enhanced	Organisations are required to achieve "**ENHANCED**" level for some or all categories. This occurs when The type, quality or quantity of data they hold, or functions performed, expose them to a significantly **HIGH** level of risk they are exposed to as per the reviewed Risk Assessment performed in line with controls described in section (5). **Or**, As part of their Continuous Improvement cycle directed towards achieving compliance to HISS.

Table 3: Organization and Control Categories

Organisations are required to attain at least the "Essential" level for each section described as per this standard before getting on boarded to DHA's NABIDH HIE Platform.

The controls or procedures defined for each section is listed for three types of users/hierarchies for a health care provider's organization:

Organization Category	Category Indicator(s)
Management	Users at this level in an entity, are those, whose primary job responsibility is to monitor activities of subordinates as well as the day to day operations or own the responsibility of overseeing a properly managed and implemented Health Information security program/management system and reviewing risk assessment reports
Administrative	Users responsible for managing/supporting/administering the systems deployed
End Users	The users who are consuming the services and working towards achieving health care provider's objectives

Table 4: Organization and Control Categories

18.6. Health Information Security Framework

Health Information security Framework (HISS) is broadly divided in to 3 sections: Applicable Legislative requirements (lists the legal & regulatory requirements the health care provider must comply for operating their facilities in the Emirate of Dubai); Governance, and NABIDH Health Information Security Framework. Details of HISS framework is presented on table below.

<table>
<tr><th colspan="4">Applicable Legislative requirements</th></tr>
<tr><th colspan="2">DESC ISR</th><th colspan="2">HRS Legislations</th></tr>
<tr><th colspan="3">NABIDH Information Security Framework</th><th>Governance</th></tr>
<tr><td>Organization of Information Security</td><td></td><td>Access Control</td><td rowspan="11">AUDIT
(Independent Validation / Verification)</td><td rowspan="2">DHA
NABIDH
HISS
Compliance</td></tr>
<tr><td>• Internal Organization</td><td></td><td>• User Access control
• Business requirements of access control
• User responsibilities
• System and application access control</td></tr>
<tr><td>Information Security Policies</td><td></td><td>System Acquisition, Development and Maintenance</td><td rowspan="9">HRS
Policies</td></tr>
<tr><td>• Management of Information Security</td><td></td><td>• Security requirements of Information systems
• Security in development, support and test processes</td></tr>
<tr><td>Assets Management</td><td></td><td>Information Security Incident Management</td></tr>
<tr><td>• Responsibility of Assets
• Classification
• Handling</td><td></td><td>• Management of Information security incidents and continuous improvement</td></tr>
<tr><td>Human Resource Security</td><td></td><td>Information Security Aspects Of Business Continuity</td></tr>
<tr><td>• Prior to employment
• During Employment
• Termination/Change</td><td></td><td>• Information Security continuity
• Cyber Resiliency</td></tr>
<tr><td>Physical & Environmental Security</td><td></td><td>Compliance</td></tr>
</table>

Applicable Legislative requirements			
DESC ISR		**HRS Legislations**	
NABIDH Information Security Framework			**Governance**
• Secure areas • Equipment Security		• Compliance to contractual and Legal requirements • Review of Information security activities	
Communications Security		**Cryptography**	
• Network Security Management • Information Transfer		• Cryptographic controls	
Operations Security		**Supplier Relationship**	
• Operation Procedures and responsibilities • Protection from Malware • Control of Operational software • Backup • Technical vulnerability management		• Information security in Supplier relationships • Supplier service delivery management	
Electronic Bio-Medical Devices		**Mobile Device Working**	
		• Mobile device security • Remote or Teleworking	
		Cloud Computing	
		• Cloud computing controls • Hosted solutions	

Table 5: Health Information Security Framework

18.6.1. Domains of NABIDH Health Information Security Framework

The framework is subdivided into 17 key domains for the organization of Health Information security that are listed below:

18.6.1.1. Domain 1: Organization Of Information Security

18.6.1.2. Domain 2: Information Security Policies

18.6.1.3. Domain 3: Assets Management

18.6.1.4. Domain 4: Human Resource Security

18.6.1.5. Domain 5: Physical & Environmental Security

18.6.1.6. Domain 6: Communications Security

18.6.1.7. Domain 7: Operations Security

18.6.1.8. Domain 8: Access Control

18.6.1.9. Domain 9: System Acquisition, Development And Maintenance

18.6.1.10. Domain 10: Information Security Incident Management

18.6.1.11. Domain 11: Information Security Aspects Of Business Continuity

18.6.1.12. Domain 12: Audit & Compliance

18.6.1.13. Domain 13: Cryptography

18.6.1.14. Domain 14: Supplier Relationship

18.6.1.15. Domain 15: Mobile Device Working

18.6.1.16. Domain 16: Electronic Bio-Medical Devices

18.6.1.17. Domain 17: Cloud Computing

18.6.1.1. Domain 1: Organization of Information Security

a. Objective

(i) To establish a management framework to develop, initiate and control the implementation and subsequent operation of information security within the HealthCare Facilities.

(ii) To explain/define to all HealthCare Facilities, the responsibility for managing information security requirements needs.

(iii) To make sure all staff will be aware of the security responsibility undertaken by the nominated security officer in the healthcare facility.

b. Policy requirements

HealthCare facilities are required to develop policies in order to research, consider, approve, formally document, audit, regularly review and enforce procedures to address:

(i) Setting the information security roles and responsibilities.

(ii) Segregation of duties

(iii) Contact with external authorities

(iv) Contact with information security interest groups

(v) Information security in business requirements.

c. Procedures

(i) Essential procedures

Responsibility	Procedure description
Management	• Information security officer responsibility is formally assigned. • Practical segregation of duties, requirements and opportunities are identified and applied. • Information security principles are incorporated into business requirements.
Administrative	No additional requirements in this section
End Users	No additional requirements in this section

Table 6: Organization of Information Security – Essential Procedures

(ii) Intermediary procedures

Responsibility	Procedure description
Management	• Establish clear lines of responsibility for information security. • Ensure the information security officer responsibility is not assigned to a position with IT operational responsibilities, such as an IT administrator. • If feasible, the information security officer should report through a risk, compliance or to a Steering Committee, or to other appropriate division of the HealthCare Facilities outside of IT. • The information security officer should understand the HealthCare Facilities's accepted risk tolerance. They should work towards implementing information security requirements that are in line with the accepted risk tolerance, while complying with required legislation, regulation or other requirements. • Detailed segregation of duties requirements and opportunities are identified, applied and monitored. • Maintain appropriate contacts with relevant authorities within the field of information security. • Identify key contacts of certain security and judicial authorities to be contacted in the cases of information security incidents, breaches, etc. • Maintain interactions and/or memberships with information security interest groups, forums and associations, in order to keep up-to-date information in the field of information security.
Administrative	No additional requirements in this section
End Users	No additional requirements in this section

Table 7: Organization of Information Security – Intermediary Procedures

(iii) Enhanced procedures

Responsibility	Procedure description
Management	The information security officer role is assigned to an executive within the governance/management group, excluding the CIO or equivalent.
Administrative	No additional requirements in this section
End Users	No additional requirements in this section

Table 8: Organization of Information Security – Enhanced Procedures

18.6.1.2. Domain 2: Information Security Policies

a. Objective

To set the strategic direction for information security in HealthCare Facilities through documented information security policies.

b. Policy requirements

Information security policies have to address requirements created by:

(i) HealthCare Facilities strategy.

(ii) Regulations, legislation and contracts.

(iii) Current and projected information security threat environment.

(iv) Some consolidation of policies may be warranted depending on the mix of individual organizational security risks and requirements.

c. Procedures

(i) Essential procedures

Responsibility	Procedure description
Management	• HealthCare Facilities must have an information security policy to meet the needs of their organisation, that is reviewed and updated at least annually and/or along with any changes that the HealthCare Facilities might undergo. • The information security policy must address security principles, security responsibilities, and an 'acceptable use policy' for protecting any organisation technology equipment, systems, resources and data. • An information security policy document must be approved by management and published, reviewed and communicated regularly to all employees and relevant external parties.
Administrative	Ensure that all employees and relevant external parties are aware of the information security policy and kept informed of any changes and updates.
End Users	Read, understand and follow obligations under the information security policy.

Table 9: Information Security Policies – Essential Procedures

(ii) Enhanced procedures

Responsibility	Procedure description
Management	No additional requirements in this section
Administrative	No additional requirements in this section
End Users	No additional requirements in this section

Table 10: Information Security Policies – Enhanced Procedures

Domain 3: Assets Management

a. Objective

(i) Identify assets belonging to the HealthCare Facilities and define and allocate responsibilities for the protection of these assets.

(ii) Ensure assets receive protection based on their importance to the HealthCare Facilities.

(iii) Ensure assets are continuously maintained to an appropriate security baseline that minimizes their vulnerabilities and threat exposure, such as regular patching and other activities (see also 18.6.1.7. – Domain 7: Operations Security).

(iv) Prevent unauthorized disclosure, modification or destruction of information stored on assets.

(v) Ensure assets are controlled and managed in accordance with best industry practice.

b. Policy requirements

A suitable high-level policy will consider and address at least:

(i) Responsibility for assets.

(ii) Asset classification and declassification in terms of legal requirements, value, criticality and sensitivity.

(iii) Asset storage, handling and secure disposal.

c. Procedures

(i) Essential procedures

Responsibility	Procedure Description
Management	*Responsibility for assets* • Create an inventory of information and information processing assets. • Assign ownership and custodianship of assets as they are created or transferred to the HealthCare Facilities. • Identify and document rules for the acceptable use of information and information processing assets including usage of personal devices in HealthCare Facilities's environment. • The termination process must be formalised to include the return of all HealthCare Facilities's assets issued, both physical and electronic. • Establish procedures to interpret classification labels from other organisations where information is shared. *Asset classification* • An asset classification scheme is to be provided. • Create a set of procedures for labelling information and its related assets in physical and electronic format. *Information assets handling* • Establish procedures for the storing, handling, distribution limitation and secure disposal of information and its related assets in physical and electronic format. • Identify and document a set of rules and guidelines for protecting assets against unauthorised access, misuse or corruption. • Establish procedures for the management of removable media.
Administrative	*Responsibility for assets* • Ensure assets are inventoried and classified. • Periodically review access restrictions and classification of assets. • Inform employees and external parties of the security requirements relating to the assets they use. • Control unauthorised copying/printing of information. • Add access restrictions supporting the protection requirements based on the classification of information. • Create and retain a formal record of authorised recipients of assets. • Protect both temporary and permanent copies of information. • Information assets need to be stored in a secure storage/location to reduce the risk of its data damage or loss as per their classification *Asset classification* • Label assets in accordance with predetermined and approved labelling procedures. *Information asset handling*

Responsibility	Procedure Description
	• Encrypt confidential data on removable media. • Ensure physical assets are sanitised (have information fully removed) prior to disposal. Paper or other physical media must be physically destroyed. • Log and sanitise or destroy media containing sensitive information when it is no longer needed. • Implement rules and guidelines for protecting assets against unauthorised access, misuse or corruption.
End Users	*Responsibility for assets* • Conform to acceptable use policy governing the acceptable use of information and assets including usage of personal devices in HealthCare Facilities's environment. • Justify access to personal Health Information . • Ensure data is classified correctly • Return all organisational assets on termination of employment, contract or agreement.

Table 11: Assets Management – Essential Procedures

(ii) Intermediary procedures

Responsibility	Procedure Description
Management	Identify, document and manage the asset/assets' lifecycle. (see also 18.6.1.7. – Domain 7: Operations Security)
Administrative	• Ensure to initiate the disposal process once the retention period is reached for the assets. • Store IT assets in accordance with specifications from manufacturers. • Prevent the use of media containing classified information with a system that has a security classification lower than that of the media. • Check information storage to ensure any Health Information and software is rendered non-retrievable prior to disposal or re-use.
End Users	No additional requirements in this section

Table 12: Assets Management – Intermediary Procedures

(iii) Enhanced procedures

Responsibility	Procedure description
Management	No additional requirements in this section
Administrative	No additional requirements in this section
End Users	No additional requirements in this section

Table 13: Assets Management – Enhanced Procedures

18.6.1.3. Domain 4: Human Resource Security

a. Objective

(i) To ensure employees, contractors and third-party users conform to the HealthCare Facilities's information security policy and procedures.

(ii) To ensure subject of care PHI are maintained confidentially and securely by those authorised to use it.

b. Policy requirements

All human resource policies and procedures, including relevant contractual terms and conditions, must incorporate information security requirements.

All employees, contractors and outsourced employees are aware of their obligations towards information security and that their roles and responsibilities are defined in relation to securing HealthCare Facilities's information and its processing facilities.

c. Procedures

(i) Essential procedures

Responsibility	Procedure Description
Management	Define security roles and responsibilities of employees, contractors, temporary staff and outsourced employees in alignment with the HealthCare Facilities high-level information security policy. ***Screen new staff*** Define background verification and screening process for new employees, temporary staff, outsourced employees and contractors according to the applicable laws and policies of Dubai Government in relation to their appointed task. ***Contracts & job descriptions*** • Include information security responsibilities and non-disclosure agreements in job descriptions, contracts of employment and contracts for service, and induction material. • Ensure all users receive relevant information security awareness training. ***Termination or change of employment*** Ensure adequate knowledge transfer and job handover. ***Disciplinary process*** Introduce, communicate and maintain a formal disciplinary process for employees, temporary staffs, contractors and outsourced employees responsible for information security breaches.
Administrative	• Follow documented recruiting and termination procedures for creating and removing users' access rights. • Ensure that a user's access rights are regularly reviewed and amended accordingly on changes of role and/or accountabilities within the organisation. • Ensure the return of all equipment and removal of all information security permissions on termination of employment or service contract, or on request. ***Maintain security policy documentation*** • Ensure the organisation has documentation matching current security legislative and policy requirements. • Ensure a security policy responsibility agreement is signed by all employees and contractors. ***Disciplinary Process***

Responsibility	Procedure Description
	Maintain necessary records on the security breaches and the disciplinary action taken by the management.
End Users	***During Employment*** • Act in accordance with all relevant information security policies and procedures. • Be aware of how to report an information security incident. ***Sign security policy responsibility agreement*** At the time of engagement, personnel sign a security policy responsibility agreement to show they have read, understood and accepted the information security policy. ***Exit procedures*** • Return all related assets (including hardware, software, information processing and storage devices, printed material or other hard copies) when leaving the organisation or role. • Transfer and document important knowledge about ongoing operations to the organisation during the notice period of termination. •

Table 14: Human Resource Security – Essential Procedures

(ii) Intermediary procedures

Responsibility	Procedure Description
Management	• Consider segregation of duties in HealthCare Facilities roles and responsibilities to avoid conflicts. • Ensure all parties receive regular and appropriate information security awareness education and training relevant to their job. • Authorise all role membership additions and changes, and associated information security permissions prior to implementation.
Administrative	• Implement and monitor segregation of duties in the roles and responsibilities of the HealthCare Facilities. • Conduct regular information security awareness training to all parties.
End Users	No additional requirements in this section

Table 15: Human Resource Security – Intermediary Procedures

(iii) Enhanced procedures

Responsibility	Procedure Description
Management	No additional requirements in this section
Administrative	• Ensure users have received relevant PHI security awareness training before they are provided with any information security access rights and credentials. • Periodically review the system audit trail of new users and users with recently re-assigned security roles.
End Users	Ensure personnel attend an induction course, which covers information security awareness, education and training relevant to their position accountabilities.

Table 16: Human Resource Security – Enhanced Procedures

18.6.1.4. Domain 5: Physical & Environmental Security

a. Objective

Prevent unauthorised physical or electronic access to the HealthCare Facilities's information assets and information processing facilities. This will guard against loss, damage, theft, interference or compromise of assets, and interruption to the organisation's operations.

b. Policy requirements

This policy will consider and address:

- Securing areas containing sensitive information
- Protection from environmental threats

c. Procedures

(i) Essential procedures

Responsibility	Procedure Description
Management	• Define security parameters and mechanisms on offices, data centers, and other working areas, based on criticality of such areas. • Provides employees with proper guidelines and awareness on the implemented protection controls in the working areas. • Secure areas that contain Health Information and information processing facilities by restricting or supervising physical access. • HealthCare Facilities must have controlled room(s) to hold critical computer equipment (servers, network). • Ensure there are adequate locks on all access doors. Maintain a record of who has access. • Preauthorize off-site use of equipment, software or information. • Provide secure offices, rooms and facilities and reasonable protection against damage from fire, flood, earthquake or other forms of environmental hazard. • Provide proper maintenance procedures on all information processing facilities.
Administrative	• Protect the perimeters of buildings or sites containing information processing facilities against unauthorized access using suitable control mechanism. • Implement UPS (uninterruptable power supply) systems to avoid power failures where deemed necessary. • Implement maintenance procedures for information processing facilities. • Install fire alarm system and test them regularly. • Implement and monitor closed circuit television (CCTV/surveillance camera) in identified secure areas.
End Users	• Conform to the implemented guidelines in securing work areas. • Do not leave the information assets unattended. • Do not discuss personal Health Information in a place where unauthorized users may overhear it. • Work in a secure area when necessary for the task in hand. • When working off-site, at home or in other public areas, use of portable computers and storage media must be operated in reference to section 22 - Domain 15: Mobile Device Working.

Table 17: Physical & Environmental Security – Essential Procedures

(ii) Intermediary procedures

Responsibility	Procedure description
Management	• Establish and operate a staffed reception area or other means to control physical access to the site or building. • Establish physical barriers to prevent unauthorized physical access and environmental contamination. • Make provision for private areas where sensitive information can be discussed. • All employees, contractors and external parties must be required to wear a visible form of identification. Any unescorted visitors and/or anyone not wearing visible identification must be immediately reported to security personnel. • All fire doors on a security perimeter must be alarmed, monitored and tested in conjunction with the walls to establish the required level of resistance in accordance with suitable regional and national standards. They must operate in accordance with the local fire code in a failsafe manner. • Maintain and monitor a secure physical logbook or electronic audit trail of all physical access.
Administrative	• Access rights to secure areas must be regularly reviewed and issues taken to management for action. • Control and monitor access to restricted areas electronically, e.g., via card system or camera. • Conduct proper testing and assessment periodically over all implemented environmental and physical protection controls.
End Users	Report broken or malfunctioning equipment to management.

Table 18: Physical & Environmental Security – intermediary Procedures

(iii) Enhanced procedures

Responsibility	Procedure description
Management	Information processing facilities managed by the HealthCare Facilities must be physically separated from those managed by external parties.
Administrative	Implement proper security controls over delivery and loading areas.
End Users	No additional requirements in this section

Table 19: Physical & Environmental Security – Enhanced Procedures

Domain 6: Communications Security

a. Objective

Ensure the information communicated between authorized resources are secured within and across health care providers.

b. Policy requirements

Policies are required to address at least the categories listed below:

(i) **Network Security Policy**

HealthCare Facilities shall formally document:

- Network services to govern the interconnections between its network, critical owned business information systems and other networks and information systems outside its formal boundaries
- The types of systems/devices that are not permitted on the network
- Any other prerequisite requirements that must be met before connection occurs

(ii) **Information Exchange Policy**

HealthCare Facilities shall formally document:

- The minimum technical standards for packaging and transmission of information
- The tools to be used for the transmission of information
- How information exchanged over a network is protected from interception, incorrect routing and/or loss
- How information exchanged physically is protected from unauthorized access, misuse or corruption

- Agreed requirements with external parties, relating to transferred information
- Responsibilities and liabilities in the event of information security incidents
- Classification and labelling for sensitive data
- Use of security controls such as cryptography
- Archival and retention policy for electronic messaging/ emails

(iii) **Information protection policy**

HealthCare Facilities shall formally document:

- Detection of malware during transmission
- Subject of care data leakage
- Attachment of inappropriate information
- Copying/modification and destruction

c. Procedures

(i) Essential Procedures

Responsibility	Procedure Description

Management	**Policies, procedures and standards**
	• Create policy documents on:
	  ○ Network Security
	  ○ Information Exchange
	  ○ Information Protection
	• Ensure users:
	  ○ Are aware of their responsibilities when transmitting information
	  ○ Know the location of and can access the relevant policies, agreements and procedures
	• Ensure formal confidentiality or non-disclosure agreements are in place with external parties that has personal Health Information . The agreement(s) must cover vendors/contractors dealing with the recipient organisations and include:
	  ○ Definitions of information to be protected
	  ○ Duration of agreement
	  ○ Process for notification of leakage
	  ○ Ownership
	• Ensure formal service level agreements are in place to cover at least the main components that support the network infrastructure.
	• Ensure all agreements and policies are regularly reviewed at least yearly and updated as required.
	• Ensure appropriate electronic signatures containing legal disclaimers are used for electronic messaging.
	• Assign roles and responsibilities for network equipment management.
	• Ensure adequate/high level of network availability.
	• Establish process to publish and maintain information on the publicly accessible systems.

Administrative	• Ensure all networking devices default accounts have their passwords changed, and default account names are renamed. • Ensure all networks are sufficiently documented including documentation of updates incorporated via the change management process. • Ensure network documentation includes up to date diagrams. • Ensure access to network services and equipment follow the procedures outlined in reference to section 15 - Domain 8: Access Control. • Ensure the DHA HISS interoperability standards are followed for the exchange of Health Information within and between organisations. • Use appropriate encryption standards (Refer to section 20 - Domain 13: Cryptography), when exchanging Health Information between external parties. • Ensure only trusted devices and users can gain access to internal networks via wireless access. • Enables clock synchronization on all networking devices with agreed reference such as Universal Coordinated Time (UTC)

Responsibility	Procedure Description
	to facilitate forensic analysis, and continuously monitor its accuracy. • Terminates network connections associated with communication sessions as per the entity defined time period of inactivity. • Implement measures to ensure adequate/high level of network availability. • Implement an archival and retention procedure for electronic messaging/ emails.
End Users	• Ensure the classification and labelling for sensitive data while exchanging information. (Refer to section 10 - Domain 3: Asset Management).

Table 20: Communications Security – Essential Procedures

(ii) Intermediary Procedures

Responsibility	Procedure Description
Management	• Identify the types of communication channels and types of sites that can be used for the different types of information being transmitted. • Ensure agreements with third parties have the right to audit and monitor activities that involve information.
Administrative	• Implement technology that can monitor the status of network devices in a secure way. • Implement technology that centralises the management of access control to networking components. • Establish and maintain appropriate network security zones, allowing data flow to follow a controlled path only. • For custom-developed applications, ensure the exchange or transfer of information between systems uses the appropriate interoperability standards. • Ensure network appliances are configured to support the segregation of networks. • Provide the appropriate level of protection to devices and information.
End Users	No additional requirements in this section

Table 21: Communications Security – Intermediary Procedures

(iii) Enhanced Procedures

Responsibility	Procedure Description
Management	No additional requirements in this section
Administrative	• Document and implement tools to enable the detection and prevention of unauthorised information transfer. • Ensure the communication of personal information such as credentials are not sent via the same mechanism where more than one part exists. For example, send the username via email and the password via text – in both cases suitable encryption is required.
End Users	No additional requirements in this section

Table 22: Communications Security – Enhanced Procedures

18.6.1.5. Domain 7: Operations Security

a. Objective

(i) To ensure appropriate controls are implemented to protect the operational security and recoverability of the HealthCare Facilities applications and information processing systems.

b. Policy requirements

HealthCare Facilities are required to document a high- level policy considering and addressing the categories listed below:

(i) The HealthCare Facilities's requirements for the backup of information, software, and systems. This must include the level of protection required for the different categories of systems and the expected retention of the data being protected

(ii) Response Plan to a disaster event and where it sits in the HealthCare Facilities's business continuity plan

(iii) The removal or upgrade of unsupported legacy software

(iv) Requirements for protection against malicious software such as malware, ransomware etc.

(v) Requirements for the frequency and type of testing of information, software, and system integrity

c. Procedures

(i) Essential Procedures

Responsibility	Procedure Description
Management	• Ensure all systems have documented operating procedures that are made available to all users. • Provide regular awareness for users on the importance of protecting health care providers infrastructure from malware attack, by focusing on avoidable user behaviours. • Develop a formal policy around the installation and use of unauthorised software, and ensure technology and processes are implemented to enforce this policy. • Create an accessible and available operating procedures manual(s) that documents: o Backup and recovery procedures o System restart and recovery procedures o Equipment maintenance functions o Change management o Instructions for handling errors o Management of audit trail and system log information o Management of a security event, including a physical security breach or one associated with a malware or hacking breach • Ensure appropriate operating procedures are created, implemented and maintained to protect documents, removable storage media, printed information and system documentation from unauthorised disclosure, modification, removal and destruction. • Ensure systems are monitored and checked regularly to ensure information system problems are identified and corrected. • Ensure data is adequately backed up and stored in a protected location. • Implements a change management process that must include the following details: o Formal management approval prior to implementation o Plan and test changes before implementation o Assess all potential impacts and risks
Administrative	**Protect information, systems and networks** • Implement anti-malware and anti-virus software on all servers and workstations. Ensure it is kept up to date. • Ensure real-time malware scanning is activated and scheduled scans are run on a regular (e.g., weekly) basis. • Ensure appropriate backups (type and frequency) are implemented for each information software/system.

Responsibility	Procedure Description
	• Ensure the backup process includes type, retention, frequency, protection controls and remote storage. • Control the installation and use of unauthorised software. **Patching/firmware** • Ensure HealthCare Facilities is up to date with current threats and ensuring the correct mitigation is in place. • Ensure all critical security patches are applied as soon as practical from the date of release. **Management, monitoring and alerting** • Implement technology that can detect and prevent access to malicious websites or sites from prohibited categories. • Ensure all systems are sufficiently documented, including documentation of updates that are incorporated via the change management process. **Capacity management** Ensure there is sufficient capacity with information systems to support good system performance and reliability.
End Users	**Report problems** Be aware of the dangers of viruses and malware and report suspicious events to management immediately.

Table 23: Operations Security – Essential Procedures

(ii) Intermediary Procedures

Responsibility	Procedure Description

Management	**Operations procedures**
	Track systems and their configuration information in a configuration management database.
	
	Protect information, systems and networks
	Ensure a system and software lifecycle policy is defined in accordance with the HealthCare Facilities's risk tolerance profile.
	
	Change management
	• Establish and apply a formal process:
	  ○ To control all changes and appropriately authorise all significant changes to information and information processing systems
	  ○ For emergency changes when incidents occur
	• Ensure all change processes are reviewed regularly and updated as required.
	• Ensure back-out/recovery plans are fully documented, incorporating procedures for when a back-out/recovery is required.
	• Ensure all assets are registered in an asset management system. The system must be able to dynamically update details regularly using agent software or similar.
	• Ensure a process exists for the adoption of systems from development or project mode to operational status. This includes the development of formal documentation to enable support of the system to the agreed service levels.
	
	People management
	• Segregate access rights to reduce opportunities for misuse of information assets.

Administrative	**Information security**
	• Provide and maintain the ability to:
	  ○ Write data to portable storage media in an encrypted format
	  ○ Securely "wipe" data/information stored on hard disks before their re-use or disposal
	• Formally document operating procedures, including how to dispose media safely and how to encrypt data on portable media.
	• Ensure system documentation includes up-to-date diagrams.
	• Protect information, systems and networks.
	• Ensure archived or stored data is kept in a secured format that is retrievable.
	• Ensure adequate backup/restore computing and storage resources are available to recover all critical systems following a major event or media failure.
	• Implement a configuration control system to track versions/revisions of software implemented and their relevant documentation.
	• Non-compliance procedures (written exemptions etc.) are invoked only for short term to allow for maintenance and upgrades that will bring systems back into compliance.
	
	Patching/firmware
	• Formally assign roles and responsibilities for vulnerability management including vulnerability monitoring, assessment and coordination responsibilities.

Responsibility	Procedure Description

	• Document a formal process that outlines standard and urgent patch application, setting out the criteria that must be met before urgent patching takes place.
	• Ensure patches are deployed to a subset of devices to allow testing before deployment to all.
	• Where a vulnerability is known or identified but no patch is currently available, use other alternatives to mitigate risk (such as firewall controls to limit functionality or restrict access), and prevent execution of suspect executable files.
	• Ensure firmware on devices is updated at least yearly, with a more regular requirement if security vulnerabilities are behind the reason for the update.
	• Where devices are no longer supported and software updates are not available, a risk assessment must be performed to determine the impact of an incident and the increased vulnerability.
	
	Testing
	• Test new versions of software and features before deployment.
	• Require vendors to produce or show evidence of adequate testing, before deploying new versions and features, or provide on-site test facilities to enable pre-deployment testing to take place.
	• Develop suitable acceptance test scripts for systems during changes and upgrades to systems.
	• Document and apply clear processes for the transfer of information/software between test/development and production environments.
	• Ensure sufficient separation exists between test/development and production environments to reduce the risk of accidental changes to the production systems.
	• Ensure testing is never performed on production systems.
	• Ensure different user profiles (with permissions appropriate for the tasks) are used for operating, testing and using systems.
	• Do not allow development tools or editors to be installed onto production systems.
	• Regularly validate backups by performing an isolated recovery.
	
	Capacity management
	• Ensure critical systems have capacity management procedures.
	• Enable monitoring of capacity management to ensure performance or function is not affected by insufficient resources
	• Understand the potential effect of the forward pipeline of projects or expansion that requires resources so capacity can be managed appropriately.
	• Ensure processes exist to regularly:
	  ○ Decommission systems that are not required
	  ○ Optimise databases
	  ○ Archive data that is not accessed regularly
	• Ensure that in the event of a failure, sufficient priority and resource allocation is given for production to resume before test/development systems.
	
	Time management

Responsibility	Procedure Description

	• Enable the ability to synchronise system clock(s) to an agreed accurate time source.
	• Disable the ability to change time on the local device.
	
	Monitoring and alerting
	• Maintain and operate an ability to log and/or alert data integrity faults generated by the system.
	• Ensure logging is occurring for the following activities:
	  ○ Changes to system configuration
	  ○ The activation/deactivation of prevention systems such as malware protection
	• Deploys adequate logs analysis mechanism and places appropriate actions on faults.
	• Secures, where appropriate, logging systems and log files against unauthorized changes including alterations, deletions, and renaming of log file contents, dates and time stamps.

End Users	**Protect information** • Ensure physically stored media, in rest or in transfer, is encrypted. • Ensure data is classified correctly so the appropriate retention policy can be applied.

Table 24: Operations Security – Intermediary Procedures

(iii) Enhanced Procedures

Responsibility	Procedure Description
Management	**Operations policy** • Ensure clear service level agreements are created with the business owner(s) for each category of system/service implemented and operated by the HealthCare Facilities. • Ensure the service level agreements clearly state what constitutes an IT disruptive event for the HealthCare Facilities.
Administrative	**Monitoring/alerting** • Ensure log file information is protected for audit purposes, based on the established log tracking timeframes. • Detect and notify the asset management function of the installation of unauthorised software. • Enable logging of administrator/operator accounts and review regularly. • Perform regular checks to ensure access to systems and networks are secure, for example: penetration tests and vulnerability assessments.
End Users	No additional requirements in this section

Table 25: Operations Security – Enhanced Procedures

18.6.1.6. Domain 8: Access Control

a. Objective

(i) To Exercise sufficient control over information and therefore prevent unauthorised access.

(ii) To minimize probabilities of information leakage, tampering, loss and system compromises.

(iii) To enable Authorised users to view and process only the information they are entitled in a need to know basis.

b. Policy requirements

The HealthCare Facilities's identity and access management framework or system will define user access controls. The level of access control policy required will vary depending on the individual HealthCare Facilities.

(i) **Document Access Control Policy**

HealthCare Facilities shall formally document the following:

- **Category Essential:**

- All users of health systems have uniquely identifiable accounts assigned to them to ensure individual responsibility. Generic accounts can be used to provide access to basic desktop functions, but access to health care and administrative applications require users to logon using their user identifiable accounts
- Standard user access profiles for common job roles within the HealthCare Facilities. Formal authorization process for user

account creation/deletion and access requests/removal (this may be part of the information security policy)

- Access rights based on a 'least rights' model and 'prior to access' approval. The approver understands what they are granting access to
- Along with terms and conditions of employment, there is a mechanism to ensure users sign an agreement that covers information confidentiality and disclosure
- A process to ensure:
    - Access control policies are regularly reviewed and updated where necessary.
    - Systems and applications that require authentication (as per the access policy) have a secure log-on mechanism in place.
    - Utility programs or tools that may be capable of overriding system and application controls are restricted and tightly controlled.
- Access to all accounts used for handling and management of subject of care-identifiable information, regardless of the device used, are to be restricted to that purpose.

➢ **Category Intermediary**

- Privileged user accounts (administrator rights) are only used for the special activities requiring their use, and not for day-to-day activities or over-ride access

- External support staff are only setup with temporary access rights for a fixed period and their accounts are set to expire at the end of that period.
- External support staff accounts are separated from internal staff accounts for easier identification and management.
- Separate authorization process for the management of system or information, over standard user authorization.
- Ensure:
    - Relevant contractual or legislative obligations are met for the access to data and services, particularly for security requirements
    - Access control policies are regularly reviewed and updated where necessary

➢ **Category Enhanced**

Ensure there is segregation of the access control roles, so the same person is not performing more than one of these roles – access request, access authorization, access administration.

- **Clear desk and screen policy**

The HealthCare Facilities shall formally document a 'clear desk and screen' policy to protect paper and information on computer displays being seen by those who should not have access to the information.

- **Password Policy**

The HealthCare Facilities shall formally document:

- Enforcement of passwords to a required complexity level based on the risk profile of the information they have access to
- Password complexity for privileged accounts (administrator access) that exceeds the password complexity required by standard users
- Enforcement of password changes at regular intervals as required by the information security policy
- Prevention of reuse of previous user passwords for a defined period of time e.g., 13 months
- Enforcement of access lockout after a fixed number of incorrect login attempts
- Enforcement of access control measures (passcode etc.) on mobile devices.

c. Procedures

(i) Essential Procedures

Responsibility	Procedure Description
Management	***General procedures*** Create policy documents covering: ○ Access control ○ Clear desk and screen ○ Password management ***Audit*** • Undertake regular audits of access logs, especially for privileged accounts. • Ensure all access allocation is documented and traceable. • Have a mechanism to allow verification that the level of access granted is appropriate.
Administrative	***Maintain access rights and password policies*** • Allow users to select and change their own passwords and include a confirmation procedure to allow for input errors. • Ensure users' access rights are appropriate to their task and are authorised to removed or modified upon termination of employment or change of role. • Ensure users are only able to access the resources and services required to carry out their duties. • Ensure access to program source code is restricted. ***Password protection*** Ensure passwords are always secured and protected. ***Secure wireless networks*** Ensure any wireless access points on the internal network are secured. ***Session protection*** • Automatically close down or terminate a session after a fixed time period of user inactivity or provide a locked screensaver option where the user must re-authenticate to unlock the system. • Ensure users cannot disable the locking mechanism.
End Users	***Good password practice*** • Follow good practice in the selection and use of passwords. • Do not share or disclose passwords. • Do not keep a record of passwords using a non-secure method such as on accessible paper, in a standard file or on a mobile device. • Change your password regularly as per the password expiry standard defined in the information security policy or if you have any reason to suspect your password has been compromised/is known. • Change your user passwords when equipment has been returned to you after repair. ***Act responsibly***

Responsibility	Procedure Description
	• Read, review and understand obligations under the access control policy (such obligations may be included in the user's signed security agreement). • Accept responsibility for all access under their credentials and ensure access related to their duties (and notify if it is not). • Do not leave the computer unlocked while unattended. • Report any security breach to the appropriate stakeholder/team. • Prevent any unintended or unauthorised release of information, particularly from unattended equipment, by terminating active sessions, locking the screen or logging off when finished.

Table 26: Access Control – Essential Procedures

(ii) Intermediary Procedures

Responsibility	Procedure Description
Management	Extend the access control policy to meet policy requirement under this section.
Administrative	***Secure networks and devices*** • Password-protect and encrypt information on devices used for remote connections, including laptops, mobile devices or portable media. • Support secure access to the network. • Password information must not be communicated to users via unencrypted emails. ***Session logging*** • Configure systems to display the date and time the user last logged in to assist in identifying unauthorised use of their account. • Remove or disable utility programs that are not required. ***Password protection*** Ensure passwords are always hashed and stored in an encrypted format. ***Monitor & audit*** • Monitor for repeated account lockouts. ○ Keep an audit trail of all login attempts to the system – including successful login activity. The log should include at least user identifier, date, time, location, and duration of all user activity within an application (including view-only activity). • Allow viewing and analysis of audit trail activity by approved users. Restrict and record the ability to delete or modify log files. • Regularly review audit trails of access and activity – perform in depth audits and pay special attention to privileged accounts and external parties. ***Access control*** • Develop and operate a procedure to provide and revoke access rights at short notice, to support the requirements of backup resources and others for temporary access. • Access the internet via a firewall or centralised device that monitors use and prevents access to unwanted material. • Maintain a remote and mobile device register. ***Policy notification*** Display a logon banner that requires the user to acknowledge and accept security terms and their responsibilities before granting access to the system.
End Users	***Good password practice*** Do not use the same passwords for personal and work-related purposes. ***Act responsibly*** Comply with section 22 - Domain 15: Mobile Devices Working.

Table 27: Access Control – Intermediary Procedures

(iii) Enhanced Procedures

Responsibility	Procedure Description
Management	Extend the access control policy to meet policy requirement under this section.
Administrative	***Access control*** • Implement tests for user proximity. The request to access information must be for a record that is, for example, recent in both time (looking at reasonably current information – not 'old') and physical location (nearby geographic information). • Do not disclose system or application identifiers until log-on successful. • Applications must enable control of user access rights at each level of access, e.g. create, read, write, modify, delete and execute. ***Advanced authentication*** • Use multi-factor authentication to control access for remote users. • Where strong authentication requirements are identified, use alternatives to passwords such as biometrics, cryptography, smart cards and tokens. • Minimise access times to high-risk systems to reduce the window of opportunity for unauthorised access.
End Users	Do not use passwords that consist of words included in dictionaries.

Table 28: Access Control – Enhanced Procedures

18.6.1.7. Domain 9: System Acquisition, Development and Maintenance

a. Objective

(i) To ensure the need for HealthCare Facilities in adopting secure system and software development lifecycle management processes.

(ii) To ensure that systems and applications in use are securely managed and supported to avoid misuse of privileges and authority, reduce probabilities of information, system and application compromises.

b. Policy requirements

HealthCare Facilities shall formally document a policy for addressing their requirements for ensuring the security on any in-house developed or external party applications regarding the acquisition, development and management of information systems, including mobile applications.

c. Procedures

(i) Essential Procedures

Responsibility	Procedure Description
Management	Ensure regular maintenance of all information processing systems.
Administrative	As part of a regular maintenance cycle, apply software patches to application and systems software to manage, remove or reduce security weaknesses.
End Users	***Preserve data integrity*** Systems must have controls to ensure data input validation, checks on the loss of data integrity as a result of processing failures, message integrity and data output validation. ***Testing and test data*** • Test data must be selected carefully, protected and controlled. • System acceptance testing must include the testing of information security requirements. •

Table 29: System Acquisition, Development and Maintenance – Essential Procedures

(ii) Intermediary Procedures

Responsibility	Procedure Description
Management	***Systems maintenance*** Where an organisation lacks the internal resources to perform systems maintenance, this function must be contracted to an external party. ***Mobile applications*** Scrutinize and assess the risks associated with the terms and conditions of the health care providers of mobile applications that are downloaded from App stores. ***Certification of systems*** • Security requirements must be identified and agreed prior to the development, acquisition and/or implementation of information systems. • Promote the use of cryptography controls to achieve information security where appropriate. • Implements security sign off process to confirm the proper implementation of security controls on all information systems/applications prior to deployment.
Administrative	No additional requirements in this section
End Users	***Cryptographic keys*** Where cryptographic controls are used, keys must be protected against modification, loss, destruction and unauthorised disclosure. ***Preserve data integrity*** Systems must support data integrity audits where messages are traceable and reportable. ***Testing and test data***

Responsibility	Procedure Description
	• The access control procedures, which apply to operational application systems, must also be applied to test application systems. • The use of operational data containing personally identifiable information (particularly subject of care EID), or any other confidential information, for developer-level testing purposes is not acceptable. • If such information is used for testing purposes (for example in user acceptance test environments which require substantial volumes of data that closely resemble operational data), all sensitive details and content must be protected. • Testing is to be performed in a realistic environment to ensure a system will not introduce vulnerabilities to the HealthCare Facilities's environment and that the tests are reliable.

Table 30: System Acquisition, Development and Maintenance – Intermediary Procedures

(iii) Enhanced Procedures

Responsibility	Procedure Description
Management	***Certification of systems*** Mandate the use of cryptography controls to assist in achieving greater information security.
Administrative	***Preserve data integrity*** Operating system services must be locked down to minimise the risk of vulnerabilities and intrusions.
End Users	***Identify potential security vulnerabilities*** Regularly check reliable sources of information about technical vulnerabilities. ***Software development*** Industry best practices must be followed in all software development projects (whether internal, outsourced or purchased products) for the capture, display, processing, exchange and persistence of sensitive information. In particular: ○ The use of established code libraries, algorithms and routines to implement security features and counter known threats ○ Source code control ○ Technical reviews ○ Testing – unit, integration, compliance and user acceptance ○ Documentation – for user, business and technical audiences ○ Change control and version management ○ Deployment mechanisms ***Testing and test data*** • Separate authorisation is required each time operational information is copied to a test environment. • Operational information must be erased from a test environment immediately after the testing is complete. • The copying and use of operational information must be logged to provide an audit trail. ***Distributed and mobile applications*** In addition to all standard or normal system design requirements, ensure all distributed and mobile applications are designed with the ability to

Responsibility	Procedure Description
	tolerate communication failure. This includes off-line capabilities and duplicate or out-of-sequence response message handling.

Table 31: System Acquisition, Development and Maintenance – Enhanced Procedures

18.6.1.8. Domain 10: Information Security Incident Management

a. Objective

(i) To ensure the appropriate tools, processes and procedures are in place to detect, report and manage information security incidents.

- An information security incident may be either a security breach or malfunction. A potential security incident may also be a threat or weakness that has been identified, which may have a detrimental impact upon the business.

b. Policy requirements

The HealthCare Facilities have to formally document policies to address at least the categories listed below:

- **Security incidents**
  - Examples of security incidents
  - Roles and responsibilities in security incident reporting
- **Reporting security incidents**
  - Reporting security weaknesses
  - Learning from incidents
  - Disciplinary process

- Procedures for ensuring staff report recorded security incidents
- Recording incidents
- Dealing with minor and major security incidents.

➢ **Investigations**

- Types of investigations
- Procedures for investigating security incidents
- Conducting investigations.

c. Procedures

(i) Essential Procedures

Responsibility	Procedure Description
Management	***Incident procedures*** • Establish management responsibilities to ensure procedures for incident management are developed and communicated within HealthCare Facilities and applicable external parties. • Create and maintain procedures for incident logging, response, handling, escalation and recovery. ***Incident notification*** • Ensure all employees and contractors are aware of their responsibilities around reporting information security incidents/events/weaknesses, including whom to report and the location of the applicable policies/procedures. • Notify vendors and/or certifying bodies of failures in system security controls. • Notify all affected parties of the security incident and possible consequences e.g., loss of data integrity. • Report significant information security incidents to NABIDH ***Incident response*** • Respond to reported security events and weaknesses in a quick, effective and orderly manner. • Facilitate protection and collection of evidence related to a security event involving staff disciplinary or legal action. • Develop a policy to handle duress situations.
Administrative	***Monitoring and alerting*** • Log, alert and monitor systems/logs for significant events indicating information security breaches and weaknesses.

	Report events • Educate users, contractors and third parties in how to report security incidents. • Report any weaknesses identified and security events as they occur. • Follow instructions from management for recording and monitoring security incidents. ***Incident response*** • Implement business continuity plans if needed. • Record all information about an incident in the appropriate register. • Implement containment processes to ensure security incidents do not spread while they are being addressed. • Once all evidence is collected, use appropriate tools and procedures to restore the environment to a normal operating state.
End Users	***Report events*** Report security events and weaknesses through appropriate channels as quickly as possible and in a confidential manner.

Table 32: Information Security Incident Management – Essential Procedures

(ii) Intermediary Procedures

Responsibility	Procedure Description
Management	***Assess*** Perform vulnerability assessments to determine where weaknesses may exist, and improvements can be made. ***Incident Notification*** Notify other agencies/departments running similar technologies or who may be at risk to the same threat, if an incident occurs. ***Incident monitoring*** Develop formal event monitoring, reporting and escalation procedures to enable the types and volumes of incidents to be monitored. ***Continual improvement*** Institute a process for continual learning and developing improvements from monitoring and analysis of security incidents. ***Procedures*** Provide an anonymous mechanism for reporting suspected security issues so the person reporting can do so without fear of ramifications. ***Incident analysis*** • Develop a procedure to review any security incidents post event and provide recommendations for avoiding a similar incident in the future. • Implement improvements in process, tools or policies to reduce the likelihood of incident recurrence.
Administrative	No additional requirements in this section
End Users	No additional requirements in this section

Table 33: Information Security Incident Management – Intermediary Procedures

(iii) Enhanced Procedures

Responsibility	Procedure Description
Management	***Tasks*** Create and maintain procedures for the handling and storage of forensic incident evidence. ***Incident analysis*** • Review the information gained from security incidents to determine the cost of each incident. • Review past incidents and lesson learnt.
Administrative	The failure of critical and/or out-of-band patching is to be included in the incident response as an event.
End Users	No additional requirements in this section

Table 34: Information Security Incident Management – Enhanced Procedures

18.6.1.9. Domain 11: Information Security Aspects of Business Continuity

a. Objective

- To ensure Information security continuity are embedded in the HealthCare Facilities business continuity management systems.
- To ensure availability of information processing facilities.

b. Policy requirements

Policy requirements include identification of:

- An acceptable loss of information security on information and services.
- An acceptable time frame for full recovery of information security.
- Procedures to recover and restore information security.
- The triggers and threats which will cause the business continuity plan to be activated.

c. Procedures

(i) Essential Procedures

Responsibility	Procedure description
Management	***Information security continuity established*** • Determine requirements for information security and the continuity of information security management in a manner to reduce the impact of major disruptive events. Capture these within the business continuity management process or within the disaster recovery management process. • Establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during a disruptive event. • Verify the established and implemented information security continuity controls at regular intervals to ensure they are valid and effective during disruptive events, i.e., run a restore.
Administrative	No additional requirements in this section
End Users	No additional requirements in this section

Table 35: Information Security Aspects of Business Continuity – Essential Procedures

(ii) Intermediary Procedures

Responsibility	Procedure description

Management	***Information security continuity governance***
	• An adequate management structure is in place to prepare for, mitigate and respond to a disruptive event.
	• Incident response personnel with the necessary responsibility, authority and competence to manage an incident and maintain information security are nominated and appointed.
	
	Information security continuity planning
	Policies are to cover:
	• All information security aspects of both business continuity and disaster recovery programmes, for example: all related processes, procedures, supporting systems and tools.
	• Mechanisms to maintain existing information security controls in what may be highly adverse operating conditions.
	• An ability to operate compensating controls within a known risk.
	
	Information security continuity plan verification
	HealthCare Facilities must verify their information security management continuity by:
	• Regularly exercising and testing the:
	  ○ Functionality of information security continuity processes, procedures and controls to ensure they are consistent with the information security continuity objectives
	  ○ Knowledge and routine required to operate information security continuity processes, procedures and controls to ensure their performance is consistent with the information security continuity objectives
	• Reviewing the validity and effectiveness of information security continuity measures when information systems, information

Responsibility	Procedure description
	security processes, procedures and controls or business continuity management/disaster recovery management processes and solutions change.
Administrative	***Availability of information processing facilities*** • Information processing facilities must be implemented with redundancy sufficient to meet HealthCare Facilities's availability requirements. • Information restores are tested regularly. • Maintain and regularly check equipment to ensure its continued availability and fitness for purpose.
End Users	No additional requirements in this section

Table 36: Information Security Aspects of Business Continuity – Intermediary Procedures

(iii) Enhanced Procedures

Responsibility	Procedure description
Management	***Availability of information processing facilities*** • HealthCare Facilities must identify business requirements for the availability of information systems. Where the availability cannot be guaranteed using the existing systems architecture, redundant components or architectures must be considered. • Where applicable, redundant information systems must be tested regularly to ensure the failover from one component to another component works as intended.
Administrative	No additional requirements in this section
End Users	No additional requirements in this section

Table 37: Information Security Aspects of Business Continuity – Enhanced Procedures

18.6.1.10. Domain 12: Audit & Compliance

a. Objective

(i) To clearly define compliance and audit requirements in order to ensure effectiveness of the implemented information security controls and avoid any violations and breaches to any laws, policies, or controls.

b. Policy requirements

The HealthCare Facilities approach to meeting these requirements must be explicitly identified, documented and kept up to date for each information system.

c. Procedures

(i) Essential Procedures

Responsibility	Procedure description
Management	• Identify and document all relevant legislative statutory, regulatory, and contractual requirements, and the organisation's approach to meeting these requirements. • Regularly update documentation for each information system and for the HealthCare Facilities. In particular establish procedures to ensure: ○ Compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of copyrighted/licensed materials, software or applications ○ Records are protected from loss, destruction, falsification, unauthorised access and unauthorised release, in accordance with legislative, regulatory, contractual and business requirements ○ Privacy and protection of personally identifiable information as required in relevant legislation and regulation • Perform regular reviews for the compliance of information processing and procedures relating to the security policies, standards and any other security requirements. • Perform a risk assessment for all information systems periodically, or following significant business or technology changes to systems, contract renewals, extensions and/or vendor changes.
Administrative	• Perform regular reviews of information system security operating procedures and practices as directed. • Undertake regular security-related testing activities including but not limited to penetration (vulnerability) testing and disaster recovery testing.
End Users	• Comply with all the applicable policies and contractual agreements. • Report areas of non-compliance to management.

Table 38: Audit & Compliance – Essential Procedures

(ii) Intermediary Procedures

Responsibility	Procedure description
Management	Take legal advice on legislative requirements as necessary.
Administrative	Undertake technical compliance review.
End Users	No additional requirements in this section

Table 39: Audit & Compliance – Intermediary Procedures

(iii) Enhanced Procedures

Responsibility	Procedure description
Management	• Risk assessments applied to all projects/business cases with appropriate approval. • Undertake an independent review of the HealthCare Facilities approach to managing information security and its implementation (i.e., control objectives, controls, policies, processes and procedures for information security) at planned intervals or when significant changes occur. • Conduct and report on organisational information assets assurance processes regarding security matters (e.g., incidents, responses, issues, risks). This may include undertaking specialist internal/external audits of their environments and taking appropriate action based on findings and recommendations.
Administrative	Implement Information security controls as required by business requirements.
End Users	No additional requirements in this section

Table 40: Audit & Compliance – Enhanced Procedures

18.6.1.11. Domain 13: Cryptography

a. Objective

(i) Ensure the proper and effective use of cryptography to protect the confidentiality, authenticity, integrity and availability of information using approved cryptographic products, algorithms and protocols.

(ii) Encrypt sensitive information to secure it from outsider and insider threats.

b. Policy Requirements

Cryptographic controls and keys must be protected by policies and procedures that ensure they are implemented, continue to be used, and are decommissioned in a manner that reduces the risks of unauthorised access and misuse.

As part of developing a policy for the use of cryptographic controls, consideration should be given to the selection of appropriate encryption controls. The policy shall include:

(i) Type of Encryption for information transit

(ii) Use of VPN for application-to data connectivity

(iii) Encryption for data at rest

(iv) Consideration of the most current encryption protocols and/or standards in the solution.

c. Procedures

(i) Essential Procedures

Responsibility	Procedure description
Management	Develops, distributes and maintains a policy on the use of cryptography and key management wherever applicable (e.g. During development and maintenance of information systems/applications etc.).
Administrative	• Implements proper cryptography and key management mechanisms as required by the HealthCare Facilities. • Implements proper protection and security controls on all cryptographic keys used by the HealthCare Facilities. • Keep systems patched and up to date and give priority to critical notifications. • Ensure encryption is enabled on all equipment that is dependent on its own controls to protect itself, such as mobile devices, backups, and offsite storage. • Seek approval for disabling encryption when required for investigative purposes and reinstate encryption when that work is completed. • Do not share passwords and/or access relating to cryptographic keys with unauthorized persons.
End Users	• Report lost and stolen equipment to IT support for appropriate actions to be taken. This action may include remotely wiping or disabling the device. • Comply with any notification requirements from IT support.

Table 41: Cryptography – Essential Procedures

(ii) Intermediary Procedures

Responsibility	Procedure description
Management	• When making new purchases (software, hardware, cloud services etc.) use that time as an opportunity to have vendors and suppliers prove to you their cryptographic products are secure, in that they: ○ Treat equipment to be returned to the supplier for repair, upgrade etc. in a manner that protects any subject of care identifiable information that may still be on it ○ Provide an alert before the expiry of cryptographic keys, to allow adequate time for arrangements to be put in place for their renewal. • People with accountability for cryptographic systems ensure: ○ Security expectations for cryptography and key management are communicated for both new projects and ongoing service delivery ○ Responsibilities are clear and unambiguous for cryptographic systems and key management. This includes responsibility for planning security services that provide oversight for cryptographic systems for the out-years ○ Contracts comply with cryptographic and key management guidance by preferring solutions that will be upgradeable for the foreseeable system lifetime over one-off point-solutions ○ Recognize that transition periods where legacy cryptography and replacement solutions running side-by-side represent potentially a higher risk than running either solution alone ○ Residual security risks are taken into account when accrediting these systems ○ Equipment used to generate, store and archive keys is physically protected ○ Relevant training and awareness programs are made available for administrators and users.
Administrative	• Manage the distribution and revocation of end-user and system certificates, with a minimum of delay. • Set a minimum notification period for the renewal of any external certificate(s). • Join user groups for the products using cryptographic controls and sign up to automatic notifications and alerts. • Reduce susceptibility to downgrade attacks by removing weak security solutions from selection. Likewise, clear text should only be able to be selected for diagnostic purposes and not operational periods where live data requires protection. Systems are returned to a secure state after running diagnostics. • Implement logging and auditing of key management related activities. • Provide assurance to executive management that cryptographic systems continue to function as intended and that risks continue to be managed and minimized. This may include risk assessments and planning security services for systems for the out-years. • Treat systems used for generating and storing cryptographic keys according to the principles of a higher security classification, as those systems represent potential access to aggregated information and if compromised could undermine the separation of duties.

Responsibility	Procedure description
End Users	• Ensure familiarity with the HealthCare Facilities's policy on the usage of cryptography controls. • Seek advice on encryption from relevant support team when procuring new technology. • Ask to be briefed on encryption and key management arrangements.

Table 42: Cryptography – Intermediary Procedures

(iii) Enhanced Procedures

Responsibility	Procedure description
Management	***Establish and document a cryptographic policy*** • Define how the standards will be implemented throughout the HealthCare Facilities. • Categories the information needing to be protected and assign the relevant encryption standards. • New cryptographic products and services are to be evaluated during procurement to ensure their cryptographic protocols, algorithms, key strengths etc. are upgradable over the expected lifetime of the system(s) proposed. This is in response to a changing threat environment, exploitable vulnerabilities being discovered, and as a protection against unintended misconfiguration. • Non-upgradable cryptographic solutions are avoided, except for short lifetime disposable technologies (devices) that can be quickly decommissioned and replaced in response to an event or incident. • Cryptographic key lifetime (e.g., validity start date, validity end date, and validity period) is appropriate and key materials are fit for the renewal cycle. Keys should not normally have a validity period of more than two to three years. • Weak cryptographic capabilities when tolerated in legacy systems (supported by time-bound written exemptions etc.), are improved at the next upgrade. • Development, test and production environments have separate chains of trust to support a separation of duties. • Revoke then replace compromised cryptographic controls (protocols, algorithms and keys) in a timely manner when responding to a security event or incident.
Administrative	Reduce susceptibility to downgrade attacks by ensuring revoked and or weak solutions are not reintroduced as a result of patching and upgrades.
End Users	No additional requirements in this section

Table 43: Cryptography – Enhanced Procedures

18.6.1.12. Domain 14: Supplier Relationship

a. Objective

(i) To ensure all HealthCare facilities have policies and procedures in place to protect information exposed to third party organizations involved throughout a procurement process agreed upon within contractual agreements.

This section must be read in conjunction with 18.6.1.9. - Domain 9: System Acquisition, Development and Maintenance.

b. Policy requirements

The review and auditing of services against contractual agreements by external suppliers must be informed by the following policies:

(ii) Define and document the criteria for selecting a supplier.

(iii) Assess supplier risks.

(iv) Create a formal contract and confidentiality agreement.

(v) Establish access controls appropriate to the degree of risk identified.

(vi) Monitor compliance with all contractual terms.

(vii) Ensure that all information assets are returned, and all access rights revoked, on the termination of agreements.

(viii) Ensure information is appropriately protected.

(ix) Ensure suppliers reporting for the information security incidents.

c. Procedures

(i) Essential Procedures

Responsibility	Procedure description
Management	***Supplier relationships*** • Assess and manage business, commercial, financial, security and legal risk associated with suppliers. • Approve potential suppliers based on risk profile. • Mandate security controls to manage risks. ***Supplier agreements*** • Establish and document supplier agreements to clarify the responsibilities of all parties involved in regarding fulfilling information security requirements. • Create appropriate formal service level agreements or equivalent with penalty clauses. • Check implementation of agreements with third-party suppliers, monitor their compliance with information security requirements and manage changes to ensure security controls are operated and maintained properly.
Administrative	***Supplier relationships*** • Assess and manage technical security risks associated with suppliers. • Perform audits of third parties' services on a regular basis. ***Supplier agreements*** • Document incidents where requirements are not met. • Escalate incident reports to administrators and management.
End Users	***Supplier relationships*** Implement controls for the monitoring and auditing of information access. ***Supplier agreements*** Implement controls for monitoring the exchange of information between various parties to ensure agreed requirements are met and any risks that were not covered in the original agreement are highlighted. ***Store audit trail of system access*** Store audit trail of data accessed/modified/deleted by suppliers as necessary.

Table 44: Supplier Relationship – Essential Procedures

(ii) Intermediary Procedures

Responsibility	Procedure description
Management	***Supplier relationships*** • Appoint owners for business processes requiring suppliers. • Create a standardised process and lifecycle for managing supplier relationships. • Determine the frequency of audits. • Appoint legal representation to oversee contracts and agreements. • Assign responsibility for managing supplier relationships to an individual within the HealthCare Facilities. (e.g., contracts or commercial manager).
Administrative	***Supplier relationships*** Work with information security, risk, supply/contract management and legal teams within the HealthCare Facilities as required.
End Users	***Supplier relationships*** • Define and document the types of information accessed by different suppliers. • Handle incidents and contingencies associated with supplier access. • Provide resilience, recovery and contingency arrangements to ensure the availability of information for processing. ***Store audit trail of system access*** Monitor and maintain an audit trail of data accessed/modified/deleted by suppliers.

Table 45: Supplier Relationship – Intermediary Procedures

(iii) Enhanced Procedures

Responsibility	Procedure description
Management	No additional requirements in this section
Administrative	No additional requirements in this section
End Users	No additional requirements in this section

Table 46: Supplier Relationship – Enhanced Procedures

18.6.1.13. Domain 15: Mobile Device Working

a. Objective

(i) To ensure the security of the HealthCare Facilities's information and assets when employees are working outside the office, using mobile devices or when non-organisation devices are used to access the HealthCare Facilities's information.

b. Policy requirements

(ii) **Mobile devices (owned & non-owned)**

The use of mobile and non-organisation owned equipment for organisation business is a growing trend that must only be permitted following the development of clear and unambiguous conditions including rights over the information and images stored.

The mobile device policy must take into account the risks of the use of privately owned mobile devices or bring-your-own-device (BYOD).

Mobile devices must be physically protected. Specific procedures, taking into account legal, insurance and other security requirements of the HealthCare Facilities, must be established for cases of theft or loss of mobile devices. Most important is the protection of the information held on such devices.

(iii) **Teleworking (working outside the office)**

Teleworking refers to all forms of work outside of the office, including non-traditional work environments. This activity is commonly

referred to as telecommuting, flexible workplace, remote work and virtual work environments.

A policy for HealthCare Facilities allowing teleworking activities must define the conditions for using teleworking.

c. Procedures

(i) Essential Procedures

Responsibility	Procedure description
Management	• A policy and supporting security measures must be adopted to manage the risks introduced by using mobile devices and to protect information accessed, processed or stored at teleworking sites. • Training must be arranged for personnel using mobile devices to raise their awareness of the additional risks resulting from this way of working and the controls implemented. • Implement a BYOD policy that addresses the following issues: acceptable use, IT requirements, security requirements (applies to all devices and connections), service policy, ownership of applications on the device, ownership of data/information on the device user, requirements on the employee, lost and found procedures. • Ensure procedure for handling lost or stolen portable computing devices, storage of entity data on these devices, connectivity to HealthCare Facilities network and systems etc.
Administrative	• Implement information security controls for mobile devices in line with those adopted in the fixed use devices (laptops) to address threats raised by their usage out of the office. • Implement a process user must follow in the event of the loss of a device. • Ensure access to equipment, devices, system and facilities at teleworking sites are authenticated, and their access to HealthCare Facilities resources are authorized based on need. • Conduct regular audit of equipment, devices, system and facilities at teleworking sites.
End Users	• Care is to be taken when using mobile devices in public places, meeting rooms and other unprotected areas. • Devices carrying important, sensitive or critical information must not be left unattended and, where possible, must be physically secured.

Table 47: Mobile Device Working – Essential Procedures

(ii) Intermediary Procedures

Responsibility	**Procedure description**

Management	• Institute a policy on the implementation of mobile device management (MDM) software for all mobile devices and those used out of office.
	• Do not allow the use of jailbroken devices.
	• Establish and operate an ability to:
	  ○ Track devices
	  ○ Use appropriate file storage products
	  ○ Remotely wipe corporate information on devices in the case of theft or inappropriate use
	  ○ Implement encryption mechanisms to protect sensitive information
	  ○ Implement proper mechanisms to disable portable computing devices
	  ○ Proper data backup procedures for the portable computing devices
	  ○ Limit or restrict usage of portable computing devices to authorized users with adequate security controls
	• Regularly review, update as needed and reissue/publish the policy document. Gain formal acknowledgement of such changes from all users.

Administrative	• Enforce MDM policies that include configuration of the device, encryption of removable storage cards (SD cards in mobiles etc.), passcode enforcement, detection of jailbroken device. • Determine out-of-date operating systems and notify users to update. • Remotely wipe entire devices or selectively wipe corporate data as requested.
End Users	Be aware that sometimes only data held in certain applications – such as email – can be wiped.

Table 48: Mobile Device Working – Intermediary Procedures

(iii) Enhanced Procedures

Responsibility	**Procedure description**
Management	Implement policy defining the applications that can be used for particular purposes. For example, the use of specialist applications for things such as medical picture taking, also support attachment of that picture to the clinical record.
Administrative	• Enforcement of MDM policies. • Examine the potential for the use of micro VPN technologies where possible to prevent resident data on devices. • Secure applications for access and synchronisation of files rather than email being used as workaround.
End Users	No additional requirements in this section

Table 49: Mobile Device Working – Enhanced Procedures

18.6.1.14. Domain 16: Electronic Bio-Medical Devices

a. Objective

(i) Identify and classify the EBMD belonging to the HealthCare Facilities.

(ii) Provide mandatory and recommended controls for securing EBMDs.

(iii) Ensure EBMD(s) are continuously maintained to an appropriate security baseline

(iv) Non-electronic biomedical devices are not scoped under this standard.

b. Policy requirements

A suitable high-level policy must consider and address at least:

(i) Responsibilities for managing the EBMD(s) in the HealthCare Facilities.

(ii) Classification of EBMDs (as per the classification scheme provided in appendix 6).

(iii) Storage, handling and secure disposal of EBMD(s).

c. Procedures

(i) Essential procedures

Responsibility	Procedure Description
Management	• Ensure the classification procedures in line with the classification principles laid down in Annexure A are approved and authorized for use suitable for HealthCare Facilities EBMD environment • Procedures to request, update, store - Manufacturer Disclosure Statement for Medical Device Security – MDS2 shall be established. • The procurement process of EBMD in HealthCare Facilities shall ensure that manufacturers / Principle Vendors / Suppliers provide the following information related to the security of the EBMD before its deployment in HealthCare Facilities (s): ✓ The intended use of the device. ✓ Risk assessment report and controls put in place to protect the EBMD, including: ○ A specific list of all security risks that were considered in the design of the EBMD. ○ A statement about who conducted the risk assessment, and who approved it. ○ A statement about technical security testing that was conducted, by whom, and what the results were. ○ A specific list and justification for all security controls that were established for your device, and a justification for all controls from this standard that were omitted. ○ A traceability matrix that links the security controls to the risks that were considered. ✓ A summary describing the plan for providing validated software updates and patches as needed throughout the lifecycle of the medical device to continue to assure its safety and effectiveness. ✓ An indication whether the EBMD will be remotely accessed, and if so, which controls are in place to secure that access. ✓ A summary describing controls that are in place to assure that the EBMD software will maintain its integrity (e.g. remain free of malware) from the point of origin to the point at which that device leaves the control of the manufacturer.

Responsibility	Procedure Description
	✓ Device instructions for use and product specifications related to recommended security controls appropriate for the intended use environment (for example, anti-virus software or use of firewall).
Administrative	• Adhere and develop associated asset labelling as per the laid down procedures. • Ensure proper labelling, filing and serialization of MDS2 w.r.t each or group of EBMD(s) used in HealthCare Facilities. • Ensure Risk Assessment reports from the procurement process are reviewed and available readily for reference.
End Users	No additional requirements in this section

Table 50: Electronic Bio-Medical Devices – Essential Procedures

(ii) Intermediary procedures

Responsibility	Procedure description
Management	No additional requirements in this section
Administrative	No additional requirements in this section
End Users	No additional requirements in this section

Table 51: Electronic Bio-Medical Devices – Intermediary Procedures

(iii) Enhanced procedures

Responsibility	Procedure description
Management	No additional requirements in this section
Administrative	No additional requirements in this section
End Users	No additional requirements in this section

Table 52: Electronic Bio-Medical Devices – Enhanced Procedures

Domain 17: Cloud Computing

a. Objective

(i) To ensure HealthCare Facilities have security controls applied by cloud service providers to their information.

(ii) These security controls have to be applicable, clearly specified and where appropriate, are built into contractual arrangements for that service.

(iii) To ensure that security controls in HealthCare facilities as a minimum, cover the following factors:

- Transmission.
- Storage.
- Processing of information.
- Data center infrastructure (such as physical access controls, third-party or sub providers credentials, building code compliance).
- Encryption and decryption of data (where, when, how).
- Recovery of client information and /or applications by the HealthCare Facilities.
- Access to client information by third parties.

(iv) To ensure HealthCare facilities have a clear understanding of the model adopted with its attendant risks, rights and obligations as specified in a cloud computing contract, forms an essential risk management tool to support the security of information.

b. Policy requirements

A cloud security policy must be formalized and identify with at least the areas below:

(i) The classification, sensitivity and security factors of information to be stored, processed or transiting the cloud service.

(ii) The availability of information.

(iii) The cloud organization incident management, jurisdictional and contractual arrangements.

(iv) The third-party provider (inter-) dependencies and capabilities.

c. Procedures

(i) Essential procedures

Responsibility	Procedure description
Management	***Cloud sourcing*** • HealthCare Facilities shall not use cloud services or infrastructure to store, process or share information that contains Health Information outside the legal jurisdiction or geographical boundaries of the United Arab Emirates, including for CSP's Backup or Disaster Recovery purposes. • Dubai government and semi government entities shall ensure mandatory compliance with DESC CSP security standards for all CSPs offering cloud services. ***Cloud security policy*** Establish or adopt and adapt the security aspects of an existing reputable cloud security policy that addresses the HealthCare Facilities's requirements for overall cloud management process and outlines roles and responsibilities of relevant stakeholders ***Risk assessment*** Perform a security risk and assurance assessment on any cloud computing initiative as part of the HealthCare Facilities's cloud security policy. ***Sovereignty*** • Ensure through a formal agreement that the CSP has no ownership rights on the stored data regardless of the format or storage medium. • Document the considerations, assessment and method of addressing any identified sovereignty issues or risks relating to information security. ***Governance*** Ensure the provider's service level agreement and usage terms are fit for purpose and in place in relation to information security. ***Confidentiality*** Define and communicate required security controls to CSP for handling of data in accordance to the applicable laws & regulations ***Integrity***

Responsibility	Procedure description
	Ensure through a formal agreement to address the security requirements for change management process. ***Availability*** • Proper cloud security controls are implemented by CSP, addressing HealthCare Facilities's requirements for periodic testing of continuity and disaster recovery plans. • Adequate measures and processes to support data portability in place whenever the HealthCare Facilities decides to move its data. ***Incident response/management*** Confirm effective incident management and response processes for information security are in place. (see also section 17 – Domain 10: Information Security Incident Management)
Administrative	• Ensure adequate cloud security controls are implemented by CSP as per architecture and deployment model approved by the entity. • Conduct periodic reviews or audits to verify CSPs' compliance with the applicable security policies and contractual requirements.
End Users	On an ongoing basis report on unusual operational security aspects that affect the ability of the user to operate in the stated policy areas.

Table 53: Cloud Computing – Essential Procedures

(ii) Intermediary procedures

Responsibility	Procedure description
Management	***Cloud sourcing*** • Select a provider who complies with the information security policy by undertaking a formal request for proposal process. • Ensure that CSPs are certified as per the CSP security standard's certification process outlined by DESC. ***Sovereignty*** • Formally identify and assess CSPs storage/processing sites for information. This may include proposed back-up and replication sites/locations. • Review other legislation/regulation as well as the cloud computing health care provider's access request processing protocols. ***Governance*** Ensure the supplier service delivery assessment includes evidence around commercial integrity, resiliency, reliability and longevity as well as compliance to security practices. ***Confidentiality*** • Confirm the cloud computing organisation operates an appropriate (role based) identity access management system. • Confirm the cloud computing organisation protects HealthCare Facilities Health Information appropriately, such as the provision/enabling of approved encryption of data at rest and in transit. ***Integrity*** • Identify and assess the operating environment, employment procedures, and physical and systems security assertions made by the selected CSP. • Confirm agreed record destruction processes are in place. ***Availability*** Identify and assess service level agreement availability specifications. ***Incident response/management*** Identify and assess service level agreement incident specifications.
Administrative	On an ongoing basis, the system is to record and report significant variances in or changes to or within the operation of the policy areas.
End Users	No additional requirements in this section.

Table 54: Cloud Computing – Intermediary Procedures

(iii) Enhanced procedures

Responsibility	Procedure Description
Management	• Ensure that the cloud service provider applies OS and Applications security hardening best practices. • Ensure that the cloud service provider applies periodic penetration testing and that a remediation program is defined, and it includes fixing the vulnerabilities based on priority. All vulnerabilities shall be prioritized and must be fixed and patched within SLAs.
Administrative	No additional requirements in this section.
End Users	No additional requirements in this section

Table 55: Cloud Computing – Enhanced Procedures

19. SECTION 9: Clinical Data Coding Terminology Standards

19.1. Purpose

19.1.1. To assure provision of the highest levels of access, quality, health status and efficiency in health sector in the Emirate of Dubai.

19.1.2. To assure facilitating the efficient flow and exchange of information among subject of care, healthcare providers, funders and health regulators with a focus on transparency and confidentiality and a balance between standardization and autonomy.

19.1.3. To assure widespread adoption of NABIDH HIE.

19.2. Scope/ Applicability

19.2.1. Providing necessary NABIDH standards for implementing and managing HIE among DHA licensed healthcare providers in the Emirate of Dubai.

19.2.2. These NABIDH standards are applicable to HealthCare Facilities in all DHA licensed health facilities of public and private sector in the Emirate of Dubai to achieve widespread adoption of HIE.

19.3. Standard statement:

19.3.1. Standardized nomenclatures and code sets used to describe clinical problems and procedures, medications, and allergies.

19.3.2. All HealthCare Facilities have to be in compliance with NABIDH Published standards.

Standard	Name of the standard	Publisher	Standard for	HealthCare Facilities Required/ Optional
ICD 10-CM (2012)	International Classification of Diseases, 10th Revision, Clinical Modification	CMS & NCHS	Diagnosis/Disease Coding	Required
CPT 4 (2012)	Current Procedural Terminology	AMA	Procedures - medical, surgical, and diagnostic services	Required
HCPCS Level II (2012)	Healthcare Common Procedure Coding System Level II	CMS & AMA	Supplies, Disposable and Consumables	Required
CDT (2011-2012)	Current Dental Terminology	ADA	Dental procedures and related services	Required
UNS (2018)	Universal Numbering System (Dental)	ADA	Observations to a specific tooth	Required
DDC	Dubai Drug Code	DHA	Drugs and related (medications)	Required
LOINC	Logical Observation Identifiers Names and Codes	RI	Laboratory and Clinical Observations	Optional
SNOMED CT (2013)	Systematized Nomenclature of Medicine Clinical Terms	IHSTDO	Comprehensive clinical granularity, used to capture problem list, allergies, diagnosis, procedures etc.	Optional
RxNorm	“normalized” notations for clinical drugs	NLM	Clinical drugs and drug delivery devices	Optional
IR-DRG	International Refined Diagnosis Related Groups	CMS	Hospital coding/Inpatient hospital payment	Optional
CVX	Clinical Vaccines Administered	IISSB	The type of product used in an immunization	Optional

Table 56: NABIDH recommended Clinical Data/Coding Terminology Standards

20. SECTION 10: Interoperability and Data Exchange Standards

20.1. Purpose

20.1.1. To assure provision of the highest levels of access, quality, health status and efficiency in health sector in the Emirate of Dubai.

20.1.2. To assure facilitating the efficient flow and exchange of information among subject of care, healthcare providers, funders and health regulators with a focus on transparency and confidentiality and a balance between standardization and autonomy.

20.1.3. To assure widespread adoption of NABIDH HIE.

20.2. Scope/Applicability:

20.2.1. Providing necessary NABIDH standards for implementing and managing HIE among DHA licensed healthcare providers in the Emirate of Dubai.

20.2.2. These NABIDH standards are applicable to Healthcare Facility in all DHA licensed health facilities of public and private sector in the Emirate of Dubai to achieve widespread adoption of HIE.

20.3. Standard statement:

20.3.1. Standards used to share clinical information such as clinical summaries, prescriptions, and structured electronic documents.

20.3.2. All HealthCare Facilities have to be in compliance with NABIDH Published standards.

Standard	Name of the standard	Publisher
HL7 V2.x	Health Level Seven Version 2.x	HL7 International
HL7 V3	Health Level Seven Version 3	HL7 International
HL7 CDA R2	HL7 Clinical Document Architecture Release 2	HL7 International
HL7 FHIR R4	HL7 Fast Healthcare Interoperability Resources Release 4	HL7 International

Table 57: NABIDH recommended Interoperability and Data Exchange Standards

21. SECTION 11: Technical and Operational Standards

21.1. Purpose

21.1.1. To assure provision of the highest levels of access, quality, health status and efficiency in health sector in the Emirate of Dubai.

21.1.2. To assure facilitating the efficient flow and exchange of information among subject of care, healthcare providers, funders and health regulators with a focus on transparency and confidentiality and a balance between standardization and autonomy.

21.1.3. To assure widespread adoption of NABIDH HIE.

21.2. Scope / Applicability

21.2.1. Providing necessary NABIDH standards for implementing and managing HIE among DHA licensed healthcare facilities in the Emirate of Dubai.

21.2.2. These NABIDH standards are applicable to Healthcare Facilities in all DHA licensed of public and private sector in the Emirate of Dubai to achieve widespread adoption of NABIDH HIE.

21.3. Standard statement:

21.3.1. Standards provide a framework for understanding the concept of clinical data and how it can be moved between systems without losing meaning or context.

21.3.2. All Healthcare Facilities have to be in compliance with NABIDH Published standards.

Standard/Type	Description	Publisher
ADT^A01	A01-Admit Subject of care Notification	HL7 International
ADT^A02	A02-Subject of care Transfer Event	HL7 International
ADT^A03	A03-Discharge event	HL7 International
ADT^A04	A04-Register a subject of care	HL7 International
ADT^A05	A05-Pre-Admit a subject of care	HL7 International
ADT^A06	A06-Change Outpatient to Inpatient	HL7 International
ADT^A07	A07-Change Inpatient to Outpatient	HL7 International
ADT^A08	A08-Update subject of care information	HL7 International
ADT^A09	A09-Subject of care departed – tracking	HL7 International
ADT^A10	A10-Subject of care arrived – tracking	HL7 International
ADT^A11	A11-Cancel admit subject of care notification	HL7 International
ADT^A12	A12-Cancel subject of care transfer event	HL7 International
ADT^A13	A13-Cancel discharge event	HL7 International
ADT^A17	A17-Swap subject of cares	HL7 International
ADT^A20	A20-Bed status update	HL7 International
ADT^A21	A21-Subject of care goes on a "leave of absence"	HL7 International
ADT^A23	A23-Delete a subject of care record	HL7 International
ADT^A25	A25-Cancel pending discharge	HL7 International
ADT^A27	A27-Cancel pending admit	HL7 International
ADT^A28	A28-Add subject of care information	HL7 International
ADT^A29	A29-Delete person information	HL7 International
ADT^A30	A30-Merge subject of care information (subject of care ID only)	HL7 International
ADT^A31	A31-Update subject of care information	HL7 International
ADT^A39	A39-Merge subject of care (subject of care ID)	HL7 International
ADT^A40	A40-Merge Subject of care (Subject of care Identifier List)	HL7 International
ADT^A45	A45-Move visit information (visit number)	HL7 International

Standard/Type	Description	Publisher
ADT^A47	A47-Change Subject of care Identifier List	HL7 International
IHE-ATNA	Audit Trail and Node Authentication	IHE International
IHE-BPPC	Basic Subject of care Privacy Consents	IHE International
IHE-CT	Consistent Time	IHE International
IHE-PDQ	Subject of care Demographics Query (ITI-47)	IHE International
IHE-PIX	Subject of care Identifier Cross Referencing (ITI-45)	IHE International
IHE-XCA	Cross-Community Access	IHE International
IHE-XCPD	Cross Community Subject of care Discovery	IHE International
IHE-XDS	Cross-Enterprise Document Sharing (ITI-18, ITI-43)	IHE International
IHE-XUA	Cross-Enterprise User Assertion	IHE International
MDM^T02	T02 – Original document notification and content	HL7 International
MDM^T04	T04 – Document status change notification	HL7 International
MDM^T11	T11 – Document cancel notification	HL7 International
ORM^O01	O01 – Used for medication orders	HL7 International
ORU^R01	R01 – Unsolicited Transmission of an Observation Message	HL7 International
RDE^O11	O11 – Pharmacy / treatment encoded order	HL7 International
VXU^V04	V04 – Unsolicited vaccination record update	HL7 International

Table 58: NABIDH recommended Technical and Operational Standards

22. REFERENCES

1) American Health InformationManagement Association (AHIMA) -- Health Information101. Available at: https://www.ahima.org/careers/healthinfo (accessed 15/05/2020)
2) Caccine administered code set (CVX) details. Available at : https://www2a.cdc.gov/vaccines/iis/iisstandards/vaccines.asp?rpt=vg (accessed 23/06/2020)
3) Camden Health Information Exchange (HIE). Available at: https://camdenhealth.org/connecting-data/hie/hie-participants/ (accessed 23/06/2020)
4) Clinical Document Architecture (CDA) standard developed by Health Level 7 International (HL7), HL7 CDA R2 details. Available at: https://www.hl7.org.uk/standards/hl7-standards/cda-clinical-document-architecture/ (accessed 23/06/2020)
5) Clinical Vaccines Administered (CVX) reference: https://www2a.cdc.gov/vaccines/iis/iisstandards/vaccines.asp?rpt=vg (accessed 23/06/2020)
6) Code on Dental Procedures and Nomenclature (CDT) details. Available at: https://www.ada.org/en/publications/cdt (accessed 23/06/2020) https://en.wikipedia.org/wiki/Current_Dental_Terminology (accessed 23/06/2020)
7) Current and Historical Interoperability Standards Advisory (ISA) Publications for Office of the National Coordinator for Health IT. A single list of available standards to be a helpful resource to improve healthcare through interoperability. Available on: https://www.healthit.gov/isa/isa-publications (accessed 23/06/2020)
8) Current Procedural Terminology, 4th Edition (CPT 4) details. Available at: https://www.cms.gov/Medicare/Coding/MedHCPCSGenInfo/HCPCS_Coding_Questions (accessed 23/06/2020)
9) DHA- Information Security Policies and Procedures. Available at: http://mydha.dha.gov.ae/sites/itd/Lists/Policies%20and%20Procedures/Forms/AllItems.aspx (accessed 19/05/2020)
10) DHA's Coding Guidelines Document Available at: https://www.eclaimlink.ae/downloads/CodingGuidelines.pdf (accessed 23/06/2020)
11) DHA's Health Information Interoperability Standards document Available at: https://www.dha.gov.ae/Documents/opendata/Health%20Information%20Interoperability%20Standards_Version1.0.pdf (accessed 23/06/2020)

12) Digital certification policy – Clinical Connect Health Information Exchange. https://ucarecdn.com/a350d277-dd14-4f0a-939c-faa5868ace33/-/inline/yes/ (accessed 23/06/2020)
13) Digital Identity Guidelines: Authentication and Lifecycle Management. Available at: https://csrc.nist.gov/publications/detail/sp/800-63b/archive/2017-06-22 (accessed 23/06/2020)
14) Digital Imaging and Communications in Medicine (DICOM) standards. Available at: https://www.dicomstandard.org/ (accessed 23/06/2020)
15) Dubai cyber security strategy. Available at: https://desc.dubai.ae/desc/ (accessed 23/06/2020)
16) Dubai data law: Law No. (26) of 2015 on the Organization of Dubai Data Publication and Sharing. Available at: https://www.smartdubai.ae/docs/default-source/dubai-data/data-dissemination-and-exchange-in-the-emirate-of-dubai-law_2015.pdf?sfvrsn=46ac2296_6#:~:text=This%20Law%20will%20be%20cited,in%20the%20Emirate%20of%20Dubai%22.&text=the%20purpose%20of%20its%20interpretation,the%20Arabic%20text%20will%20prevail. (accessed 10/05/2020)
17) Dubai Data Policies of 2017. Available at: https://www.smartdubai.ae/ResourcePackages/ Theme/assets/dist/docs/ Dubai%20Data%20Policies%20En.pdf (accessed 23/06/2020)
18) Dubai cyber security strategy (2019). Available at: https://desc.dubai.ae/ (accessed 23/06/2020)
19) Dubai Data Manual: Version 3.0 (November 2016). Published by the Smart Data Establishment. Available at: https://www.smartdubai.ae/docs/default-source/dubai-data/dubai-data-policies-en.pdf?sfvrsn=b2019ec4_6 (accessed 10/05/2020)
20) Dubai Drug Code (DDC) details. Available at: http://www.isahd.ae/content/docs/GC%2012-2018%20The%20Dubai%20Drug%20Code%20(DDC)%20List%20and%20eClaimLink%20System.pdf (accessed 23/06/2020)
21) Dubai Electronic Security Center (DESC) Law No 11 of 2014. Available at: https://desc.dubai.ae/ (accessed 19/08/2020)
22) Dubai Medical Coding Guidelines. Available at: https://www.eclaimlink.ae/downloads/CodingGuidelines.pdf (accessed 23/06/2020)
23) Dubai's e-claim link Codes and Lists. Available at: https://www.eclaimlink.ae/dhd_codes.aspx (accessed 23/06/2020)
24) ENV 13608-1:2000 Health Informatics - Security For Healthcare Communication - Part 1: Concepts And Terminology. Available at:

https://standards.iteh.ai/catalog/standards/cen/64818ee4-1478-4b71-87d6-a8aa95c82021/env-13608-1-2000 (accessed 23/06/2020)

25) General Data Protection Regulation (GDPR) consent guidance. Available at: https://iapp.org/resources/article/consultation-gdpr-consent-guidance/(accessed 23/06/2020)

26) Guide to Privacy and Security of Electronic Health Information– Office of the National Coordinator for Health Information Security. Available at: https://www.healthit.gov/topic/health-it-resources/guide-privacy-security-electronic-health-information (accessed 23/06/2020)

27) HCPCS Level II details. Available at: https://www.cms.gov/Medicare/Coding/MedHCPCSGenInfo/HCPCS_Coding_Questions (accessed 23/06/2020)

28) Health Level Seven International Version 2 (HL7's V2) messaging standard. Available at: https://www.hl7.org/implement/standards/product_brief.cfm?product_id=244 (accessed 23/06/2020)

29) Health Level Seven International Version 3 (HL7 V3) details. Available at: https://www.hl7.org.uk/standards/hl7-standards/hl7-v3/ (accessed 23/06/2020)

30) Healthcare Common Procedure Coding System (HCPCS Level II) reference: https://www.cms.gov/Medicare/Coding/MedHCPCSGenInfo/HCPCS_Coding_Questions (accessed 23/06/2020)

31) HL7 Fast Healthcare Interoperability Resources (FHIR) details. Available at: http://hl7.org/fhir/summary.html (accessed 23/06/2020)

32) Integrating the Healthcare Enterprise (IHE) Profiles details. Available at: https://www.ihe.net/resources/profiles/ (accessed 23/06/2020)

33) International Classification of Diseases, Tenth Revision, Clinical Modification (ICD-10-CM) details. Available at: https://searchhealthit.techtarget.com/definition/ICD-10-CM (accessed 23/06/2020)

34) International Organization for Standardization. Available at: https://www.iso.org/ (accessed 23/06/2020)

35) International Refined Diagnosis Related Groups (IR - DRG 2015) details. Available at: https://www.eclaimlink.ae/docs/Payment%20Parameter%20Calculation%20Presentation.pdf (accessed 23/06/2020)

36) Interoperability Standards Advisory Office of the National Coordinator for Health IT. Available at: https://www.healthit.gov/isa/isa-publications (accessed 23/06/2020)
37) Ireland Health service IT Security Policies. Available at: https://www.hse.ie/eng/services/publications/pp/ict/ (accessed 23/06/2020)
38) Logical Observation Identifiers Names and Codes (LOINC) details. Available at: https://loinc.org/about/ (accessed 23/06/2020)
39) New York Care Information Gateway. Available at: https://www.nyehealth.org/glossary/ny-care-information-gateway/ (accessed 23/06/2020)
40) Normalized notations for clinical drugs (RxNorm) reference: https://searchhealthit.techtarget.com/definition/RxNorm(accessed 23/06/2020).
41) Prescription for Electronic Drug Information Exchange (RxNorm) details. Available at: https://searchhealthit.techtarget.com/definition/RxNorm (accessed 23/06/2020)
42) Privacy and Security Requirements and Considerations for Digital Health Solutions. Available at: https://infoway-inforoute.ca/en/ (accessed 23/06/2020)
43) Saudi National E- Health Strategy - Managing Change. Available at: https://www.moh.gov.sa/en/Ministry/nehs/Pages/Managing-Change.aspx (accessed 23/06/2020)
44) Systematized Nomenclature of Medicine -- Clinical Terms (SNOMED CT) details. Available at: http://www.snomed.org/snomed-ct/five-step-briefing (accessed 23/06/2020)
45) The Executive Council of Dubai Government Resolution No. (13) of 2017 for Information Security Regulation in Dubai Government. Available at: http://www.internalauditor.me/article/information-security-regulation-isr-whats-changed-and-why-its-important/ (accessed 10/05/2020)
46) The HITRUST Common Security Framework. Available at: https://hitrustalliance.net (accessed 10/05/2020)
47) The Interoperability Standards Advisory (ISA) 2019 - Reference Edition (published January 2019): https://www.healthit.gov/isa/sites/isa/files/inline-files/2019ISAReference Edition.pdf (accessed 23/06/2020)
48) The Interoperability Standards Advisory (ISA) 2020 - Reference Edition (published December 2019): https://www.healthit.gov/isa/sites/isa/files/inline-files/2020-ISA-Reference-Edition.pdf (accessed 23/06/2020)
49) The Universal Numbering System (UNS) details. Available at: https://radiopaedia.org/articles/american-dental-association-universal-numbering-system (accessed 23/06/2020)
50) UAE DOH policy on the Abu Dhabi health information exchange. Available at:

https://doh.gov.ae/-/media/A78104416DF2440E89AC90FB75F11055.ashx (accessed 23/06/2020)

51) UAE Federal Law No. 2 of 2019 concerning the use of information and communication technology in the area of health. Available at: https://globalcompliancenews.com/new-health-data-law-uae-20190402/#:~:text=Federal%20Law%20No. ,sensitive%20categories%20of%20data%3B%20and (accessed 23/06/2020)

APPENDIX 1: CONSENT TO Register in NABIDH Health Information Exchange

This form is to be used by subject of cares who want to register/participate in the NABIDH Health Information Exchange (HIE).

NABIDH Health Information Exchange ("NABIDH HIE") is a way of allowing your health information to be shared by participating providers meaning medical groups, hospitals, labs, radiology centers, and other health care providers through secure, electronic means. The purpose of the NABIDH is to give each of our participating providers the benefit of having access to all of your health information that is maintained by the participating providers when delivering healthcare to you.

- Your participation in the NABIDH is voluntary and your receipt of treatment or payment for treatment will not be conditioned on whether or not you sign this form.
- Your participation in NABIDH will provide you the opportunity to access your health information and results through NABIDH portal/website.
- You have the complete right to opt out of NABIDH HIE whenever you wish to.
- If you deny consent for NABIDH, your healthcare providers may not be able to access critical health information about you, obtained during a prior encounter, in a timely manner.
- Your electronic health information may be re-disclosed by an NABIDH Participant or Care Provider to others only to the extent permitted by the UAE federal laws and Emirate of Dubai regulations for the purpose of treatment, quality assurance, public health, or research. This is also true for your health information that exists in a paper form.

There are penalties for inappropriate access to or use of your electronic health information. If at any time you suspect that someone who should not have seen or gotten access to information about you has done so, call one of the NABIDH Providers; visit the NABIDH website: https://nabidh.ae or call the NABIDH at 800 DHA (800 342).

By signing this form I hereby ACKNOWLEDGE and AGREE as follows:

1. My health care providers that participate in the NABIDH HIE may disclose my health information to the NABIDH system and my health information may be shared with all health care provider participants of the NABIDH that are involved in my care in the Emirate of Dubai.

2. The NABIDH HIE may also share my health information with members of other UAE health information exchanges to which the NABIDH connects who are involved in my care (ONLY within UAE).
3. My health information that will be shared through the NABIDH will include health information from both before and after today's date.
4. My health information that will be shared through the NABIDH includes information about my diagnoses, test results (like x-rays or laboratory), and medications that have been prescribed to me.
5. Health care providers who receive health information about me through the NABIDH may copy or include my health information into their own medical records when caring for me.
6. If I cancel this consent, such cancellation will have no effect on the health information such providers already accessed and copied.
7. I understand that this consent will remain in effect until I cancel (opt out) it.
8. I understand that my refusal to sign this Consent will not prevent me from receiving care from healthcare providers or another Participant.
9. I understand that in almost all cases I have the right to inspect or copy the specific health information I have authorized to be disclosed by this Consent form.
10. I understand that I have the right to cancel this consent by completing and submitting the "NABIDH Health Information Exchange Opt-Out Request Form" and submitting the completed form to my healthcare provider.
11. It may take between 2 - 5 business days after receipt to process my consent and for the NABIDH to make my information available for sharing through the NABIDH
12. The information related to the NABIDH Consent form has been interpreted in a language that is understood by me.
13. I have a right to ask for a copy of this form after I sign it.

☐ I also agree that Nabidh users can access my sensitive health information that includes:

(m) Chemical dependency
(n) Human immunodeficiency virus (HIV), also known as Acquired Immune Deficiency Syndrome (AIDS).HIV/ AIDS status
(o) Mental health conditions
(p) Behavioral Health Information
(q) Psychotherapy Notes
(r) Alcohol and substance abuse
(s) Reproductive health
(t) Genetic testing information
(u) Sexual health (including sexually transmitted diseases).
(v) Child pregnancy data
(w) Child abuse conditions

Subject of care's Name: Last *	First*	Middle
National ID number: *	Subject of care's Date of Birth:*	Primary Phone Number: * ( )
Email:	Sex (M/F):	Secondary Phone Number: ( )
Postal Address:*	City:*	P.O Box:*
*required information		

_____ ----------

Signature of Subject of care (or Legal Representative) Date Signed
If under 18 years, signature of Parent or Guardian
Legal Representative Name * _____
Legal Representative Relationship to Subject of care* _____
Legal Representative Phone Number * _____

Fill out and return form to healthcare provider.

Contact Us: NABIDH Health Information Exchange (HIE) Division
Tel 800 DHA (800 342); Email info@dha.gov.ae ; https://nabidh.ae.

APPENDIX 2: Consent To OPT OUT from NABIDH Health Information Exchange

This form is to be used by subject of cares who want to Opt Out from the NABIDH Health Information Exchange platform in the Emirate of Dubai.

NABIDH Health Information Exchange is a way of allowing your health information to be shared by participating Providers meaning: medical groups, hospitals, labs, radiology centers, and other health care providers through secure, electronic means.

The purpose of the NABIDH is to give each of our participating providers the benefit of having access to all of your health information that is maintained by the participating providers when providing healthcare to you.

We expect that using NABIDH will provide you an excellent access to all your health Information through NABIDH portal. In addition, NABIDH will deliver faster and more complete access to your information to make better informed decisions about your care especially in emergency situations.

YOU CAN CHOOSE NOT TO PARTICIPATE (OPT-OUT).

Participation is voluntary and will not affect your ability to receive medical care. If you opt-out, the NABIDH will block access to your health information EVEN for emergency treatment. This means that it may take longer for your healthcare providers to get medical information they may need to treat you.

Even if you do not want to participate in NABIDH`s, Emirate of Dubai law reporting requirements will still be fulfilled through Public Health Registries and research. This means your health information will be used anonymously.

PLEASE NOTE: It is always good to make sure your healthcare provider knows about all of your conditions and medications even if you choose to Opt-Out of the NABIDH.

If you opt-out and later decide to reverse that decision, please contact NABIDH to sign another NABIDH registration form to cancel your opt-out. Your health information from the period during which you had opted-out WILL be available through the NABIDH after you decide to re-register again.

By signing this form, I hereby ACKNOWLEDGE and AGREE as follows:

• I understand that any of my health information received by any NABIDH or affiliate WILL NOT BE VISIBLE in the electronic medical records in which NABIDH participates. This will include in EMERGENCY CARE situations.

- I understand that I am free to revoke this Opt-Out request at any time and can do so by completing a new NABIDH Opt-In form.
- It may take between 2 - 5 business days after receipt to process this Opt-out form and to prevent the sharing of my health information.

☐ **Facility OPT OUT**: I DO NOT WANT my health information from this facility to be shared with other facility NABIDH users.

☐ **Global OPT OUT**: I DO NOT WANT my information visible within the NABIDH in which NABIDH Health participates.

Subject of care's Name: Last *	First*	Middle
National ID number: *	Subject of care's Date of Birth:*	Primary Phone Number: * ( )
Email:	Sex (M/F):	Secondary Phone Number: ( )
Postal Address:*	City:*	P.O Box:*
*required information		

_____ ----------

Signature of Subject of care (or Legal Representative) Date Signed

If under 18 years, signature of Parent or Guardian

Legal Representative Name * _____

Legal Representative Relationship to Subject of care* _____

Legal Representative Phone Number * _____

Fill out and return form to healthcare provider.

Contact Us: NABIDH Health Information Exchange (HIE) Division

Tel 800 DHA (800 342); Email info@dha.gov.ae ; https://nabidh.ae.

APPENDIX 3: Incident Prioritization

	Impact Code	Examples
1	Extensive/Widespread	An incident impacting the entire Health Information Exchange Platform OR An incident that impacts the critical business service
2	Significant/Large	An incident impacting multiple stakeholders and PHCS
3	Moderate/Limited	An incident impacting multiple individual users or PHCS
4	Minor/Localized	An incident impacting one or few users

	Urgency Code	Examples
1	Critical	An incident affecting the entire service resulting in the inability to perform/provide the functions of the service
2	High	An incident affecting the ability for a user to do work
3	Medium	An incident that moderately affects the ability for a user to do work and/or a workaround exists
4	Low	An incident that does not impede the ability to do work or provide service functions

Incident Priority Matrix		Impact			
		Extensive / Widespread	Significant / Large	Moderate / Limited	Minor / Localized
Urgency	Critical	1	1	2	3
	High	2	2	3	4
	Medium	3	3	4	4
	Low	4	4	4	5

APPENDIX 4: NABIDH Breach Notification and Incident Reporting

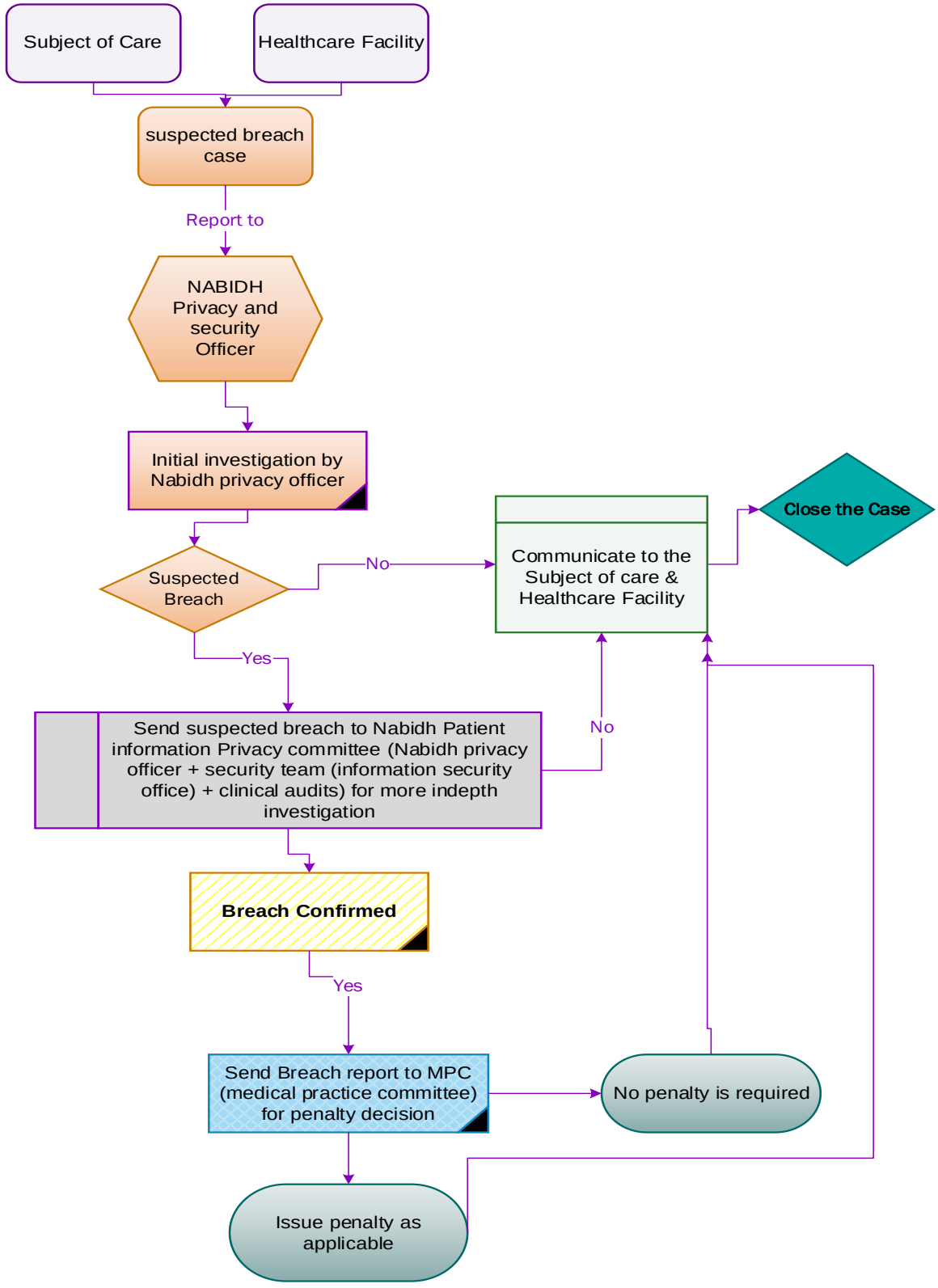

Figure 2: NABIDH Breach Notification and Incident Reporting

APPENDIX 5: NABIDH PHI Privacy Complaint and Breach Notification Form

If you have questions about this form, call 800DHA or email info@dha.gov.ae

Name	_____ **First**	_____ **Middle**	_____ **Last**
Phone	_____ Mobile	_____ Other (Home/work)	
Address			
Email			
Are you filing this complaint for someone else?	**YES**	**NO**	
If Yes, whose health information privacy rights do you believe were violated?			
_____ **First**	_____ **Middle**	_____ **Last**	
Who (or what agency or organization, e.g., provider, health plan) do you believe violated your (or someone else's) health information privacy rights or committed another violation of the Privacy Rule?			
PERSON / AGENCY / ORGANIZATION			
STREET ADDRESS			
Phone			
Email			
When do you believe that the violation of health information privacy rights occurred? **LIST DATE(S)** _____			
Describe briefly what happened. How and why do you believe your (or someone else's) health information privacy rights were violated, or the privacy rule otherwise was violated? Please be as specific as possible.			

_____			
_____			
_____			
Please sign and date this complaint. _____ _____			
DATE		**SIGNATURE**	
Filing a complaint with NABIDH is voluntary. However, without the information requested above, NABIDH may be unable to proceed with your complaint. We will use the information you provide to determine if we have jurisdiction and, if so, how we will process your complaint. Information submitted on this form is treated confidentially and is protected. Names or other identifying information about individuals are disclosed when it is necessary for investigation of possible health information privacy violations, for internal systems operations, or for routine uses, which include disclosure of information outside the Dubai Health Authority for purposes associated with health information privacy compliance and as permitted by law. It is illegal for a covered entity to intimidate, threaten, coerce, discriminate or retaliate against you for filing this complaint or for taking any other action to enforce your rights under the applicable laws. You are not required to use this form. You also may write a letter or submit a complaint electronically with the same information. To submit an electronic complaint, email to info@dha.gov.ae			
If we cannot reach you directly, is there someone we can contact to help us reach you? (optional)			
Name	_____ First	_____ Middle	_____ Last
Phone	_____ Mobile	_____ Other (Home/work)	
Address			
Email			
Have you filed your complaint anywhere else? If so, please provide the following. (Attach additional pages as needed.) (optional)			
PERSON / AGENCY / ORGANIZATION			
Phone			
Email			

Table 59: NABIDH PHI Privacy Complaint and Breach Notification Form

APPENDIX 6: Classification of Electronic Bio-Medical Devices (EBMD)

The levels used for this classification are oriented on the potential negative impact a problematic EBMD might have on the subject of care, therefore some detailed distinctions have been made:

Classification	*Level of Impact*
Class I	Low
Class I – sterile	Low-Medium
Class I – measuring function	
Class II a	
Class II b	Medium – High
Class III	High
Active implantable medical devices	High
(AIMD)	

The HealthCare Facilities must ensure that following minimum information is available from the manufacturer for determining the classification of a device using a set of classification principles, as listed in Section 25.2:

- Manufacturer's intended use of the device*
- Level of impact to subject of cares, users and other persons
- Degree of invasiveness in the human body

- Duration of use

Identical devices may be classified differently if they are to be used in different parts of the body. Therefore, the manufacturer's intended use of the device is so critical to determining the appropriate classification. The intended use should be clarified in the report card or MDS2 of the device.

Classification Principles

a. Maximum Principles

- If more than one classification rule applies, always the rule leading to the highest classification should be chosen.
- If an EBMD is used in combination with other EBMDs, each EBMD should be classified individually.
- For systems and procedure packs, the classification for the entire system or pack is the highest classification of any individual EBMD in the system or pack.

b. Devices with a measuring function

An EBMD is considered to have a measuring function if the device is intended by the manufacturer to measure:

- Quantitatively a physiological or anatomical parameter.
- A quantity or a qualifiable characteristic of energy or of substances delivered to or removed from the human body.

The measurements given by a medical device should:

- Display in UAE legal units of measurement, and
- Be accurate to enable the device to achieve its intended purpose.

Manufacturers of Class I EBMDs that have a measuring function should classify this device in the “Low – Medium” impact classification.

c. EBMDs required to be sterile

Some medical devices are required to be sterile when used to minimize the risk of infection. Such medical devices should be terminally sterilized to a Sterility Assurance Level (SAL) of at least 10^{-6}, unless this is not possible due to device material incompatibility with the proposed sterilization process. It is the responsibility of the manufacturer to determine the most appropriate method for achieving the required SAL for a particular device after due consideration of the design and construction of the device.

Devices that are required to be sterile, but cannot be subjected to terminal sterilization, can be manufactured aseptically, for example by sterile filtration. Devices manufactured in this manner have a lower SAL than those subjected to terminal sterilization. Manufacturers of Class I EBMDs that have to be sterile should classify this device in the “Low – Medium” impact classification.

d. Duration

When determining the appropriate classification for an EBMD, the manufacturer should take the account of the duration of its use, distinguishing:

Period of intended use	***Descriptive label***
Less than 60 minutes	**Transient**
At least 60 minutes, but no more than 30 days	**Short term**
More than 30 days	**Long term**

e. Non-Invasive EBMDs

- Rule 1: A non-invasive EBMD is Class I, unless the device is classified at a higher level under another rule in this clause.
- Rule 2a: A non-invasive device to modify the biological or chemical composition of blood, other body liquids, or other liquids to be infused in the subject of care is classified as Class IIb.
- Rule 2b: A non-invasive device to be used in treatment consisting of filtration, centrifugation or exchanges of gas or heat is classified as Class IIa.

f. Invasive EBMDs

(i) Transient use

- Rule 1a: Surgically invasive EBMDs for transient use to diagnose, monitor, control or correct a defect of the heart, or central circulatory system through direct contact are classified as Class III.
- Rule 1b: A surgically invasive EBMD for transient use to supply ionizing radiation is Class IIb.
- Rule 1c: A surgically invasive EBMD for transient use to have a biological effect is Class IIb.
- Rule 1d: A surgically invasive EBMD for transient use to administer medicine via a delivery system, and where the administration is potentially hazardous to the subject of care is Class IIb.

(ii) Short term use

- Rule 2a: A surgically invasive EBMD for short-term use to supply ionizing radiation is Class IIb.
- Rule 2b: A surgically invasive EBMD for short-term use to be specifically used to diagnose, monitor, control or correct a defect of the heart, or central circulatory system, through direct contact with these parts of the body is Class III.
- Rule 2c: A surgically invasive EBMD for short-term use to be used in direct contact with the central nervous system is Class III.

(iii) Long term use

- Rule 3a: Invasive EBMDs that are for long-term use are classified as Class IIb.
- Rule 3b: A surgically invasive EBMD for long-term use to be used in direct contact with the heart, the central circulatory system or the central nervous system is Class III.
- Rule 3c: A surgically invasive EBMD for long-term use intended by the manufacturer to have a biological effect is Class III.
- Rule 3d: A surgically invasive EBMD for long-term use to administer medicine is Class III.

g. Active EBMDs

- Rule 1: An active EBMD is Class I, unless the device is classified at a higher level under another rule in this clause.

(i) Therapeutic use

- Rule 2a: An active EBMD for therapy to administer energy to a subject of care, or exchange energy to or from a subject of care is Class IIa.
- Rule 2b: An active EBMD to administer or exchange energy in a potentially hazardous way, having regard to the nature, density and site of application of the energy is Class IIb.
- Rule 2c: An active EBMD to control or monitor, or directly influence the performance of an active medical device for therapy of the kind in the previous entry is Class IIb.

(ii) Diagnostic use

- Rule 3a: An EBMD to supply energy that will be absorbed by a subject of care's body (except a device that illuminates the subject of care's body in the visible spectrum) is Class IIa.

- Rule 3b: An EBMD to be used to image in vivo distribution of radiopharmaceuticals in subject of cares is Class IIa.

- Rule 3c: An EBMD used for direct diagnosis or monitoring of vital physiological processes of a subject of care, excluding devices mentioned in the previous entry is Class IIa.

- Rule 3d: An EBMD to monitor vital physiological parameters of a subject of care, and the nature of variations monitored could result in immediate danger to the subject of care is Class IIb.

- Rule 3e: An EBMD to emit ionizing radiation and to be used for diagnostic or therapeutic interventional radiology is Class IIb.

- Rule 3f: An EBMD to control, monitor or directly influence the performance of a device in the previous entry is Class IIb.

(iii) Administrative use

- Rule 4a: An active EBMD to administer or remove medicine, body liquids or other substances is Class IIa.

- Rule 4b: An active EBMD to administer or remove medicine, body liquids or other substances in a way that is potentially hazardous to the subject of care, having regard to the substances, the part of the body concerned, and the characteristics of the device is Class IIb.

h. Special Rules

(i) Recording X-Ray diagnostics

- Rule 1: A non-active EBMD to record x-ray diagnostic images such as x-ray films, photostimulable phosphor plates is Class IIa.

(ii) Active Implantable EBMDs

- Rule 2a: An active implantable EBMD is classified as Class AIMD.
- Rule 2 b: An implantable accessory to an active implantable EBMD is Class III.
- Rule 2c: An active EBMD to control, monitor.

Document Revision History

Version	Date	Type of update	Prepared/Revised by
1.0	September 1, 2020	First Release	Department of Health Informatics & Smart Health Health Regulation Sector Dubai Health Authority

Table 60: Document Revision History

Contact Us

Still have questions?

For more information on NABIDH, please reach out through the following channels:


800 DHA (800 342)


info@dha.gov.ae


https://nabidh.ae

This document was last updated on **01 Sep 2020**