دائـــــرة الـصـــحـــة
DEPARTMENT OF HEALTH

DOH POLICY ON THE ABU DHABI HEALTH INFORMATION EXCHANGE

November 2019

PUBLIC عـــام

دائـــــرة الـــصـــحـــة
DEPARTMENT OF HEALTH

Document Title:	Policy on the Abu Dhabi Health Information Exchange (HIE)
Document type	Policy
Document Ref. Number:	DOH/POL/STR/HIE/1.0/2019
Effective Date:	November 2019
Previous versions	November 2018
Document Owner:	Strategy Division
Applies to:	The entire healthcare sector of Abu Dhabi
Classification:	◉ Public
This document should be read in conjunction with related UAE laws, DOH Standards, Policies and Manuals.	

ABOUT DEPARTMENT OF HEALTH ABU DHABI (DOH)

The Department of Health (DOH), previously known as the Health Authority Abu Dhabi (HAAD) is the regulative body of the health system in the Emirate of Abu Dhabi and seeks excellence in health for the community by regulating and monitoring the health status of the population. DOH shapes the regulatory framework for the health system, inspects against regulations, enforces regulations, and encourages the adoption of Best Practices and performance targets by all health service providers. DOH also drives programmes to increase awareness and adoption of healthy living standards among the residents of the Emirate of Abu Dhabi in addition to regulating scope of services, premiums, and reimbursement rates of the health system in the Emirate of Abu Dhabi.

The health system of the Emirate of Abu Dhabi is comprehensive, encompasses the full spectrum of health services, and is accessible to all residents of Abu Dhabi. The health system encompasses providers, professionals, patients, insurers, and the regulator. Providers of health services include public and private services, and the system is financed through mandatory health insurance (with the exception to Thiqa) and has three main sources of financing: Employers or Sponsors, the Government, and Individuals. The Health Insurance scheme places responsibilities on any Insurer, Broker, Third Party Administrator, Health Provider, Employer, Sponsor (including educational establishments), Limited Income Investors, and Insured Persons to participate in the Health Insurance Scheme.

Table of Contents

Definitions and Abbreviations

Term	Definition
ADHIE	The Abu Dhabi Health Information Exchange as operated by the ADHIE Operator. Where the context requires, references to the rights and obligations of 'ADHIE' shall mean the rights and obligations of ADHIE Operator.
ADHIE Patient Portal	A secure online website that gives Patients and their personal representative's access to their Patient Data available on the ADHIE Platform.
ADHIE Platform	The electronic health information exchange platform for the Emirate of Abu Dhabi designed, developed, implemented, maintained and operated by the ADHIE Operator.
Platform Access Requirements	The requirements that each Participant must meet to access and use the ADHIE Platform as published by ADHIE Operator from time to time.
ADHIE Platform Interface Standards	The interface standards that each Participant must comply with to connect and interwork with the ADHIE Platform as published by ADHIE Operator from time to time.
ADHIE Operator	The entity that owns and operates the ADHIE Platform.
ADHIE Provider Portal	A secure online website that gives Participants access to the Patient Data that is available on the ADHIE Platform.
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.
Applicable Laws	The law no. 10, 2018 establishing DOH, the Federal Decreed Law no. 4, 2016 on the subject of Medical Liability, the Federal Law no. 2, 2019 on the usage of information technology & telecommunication in healthcare field, the Federal Law no. 5, 2019 on regulating the practice of human medicine, and their respective implementing regulations, all as amended, other all relevant enactments, regulations, regulatory policies, regulatory guidelines, policies, directions, standards, industry codes, regulatory permits and regulatory licenses, in each case, which are in force from time to time.
Audit Log	An electronic record of all access to the ADHIE Platform, such as, for example, queries made by Authorized Users, type of information accessed, information flows between the ADHIE

	Platform and Participants, and date and time markers for those activities.
Authentication	The corroboration that a person is the one claimed to be by such person.
Authorized User	An individual who has been authorized by a Participant or ADHIE to access Patient Health Information via the ADHIE Platform in accordance with the Policies.
Best Practice	The application of the best knowledge derived from accepted high quality research and respected expert experience to achieve optimum processes and outcomes.
Breach	Any unauthorized access, disclosure, acquisition or use of Patient Data, whether by Wilful Misconduct or otherwise or any breach of DOH Policies.
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.
Change of Control	That a person who had Controlled any person ceases to do so, or another person acquires Control of such a person, unless such Change of Control happens for the purpose of a solvent voluntary reconstruction or amalgamation.
Data	Any data, including any health and other information, text, radiological images, 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 Onboarding Requirements	The requirements that each Participant must comply with in making available Patient Data to the ADHIE Platform as published by ADHIE Operator from time to time.
Data Specifications	The specifications detailing the content, format and technical and security requirements for Patient Data as published by the ADHIE Operator from time to time.
Data Supplier	An individual or entity that supplies Data to or through the ADHIE. Data Suppliers include both Participants and entities that supply to, but do not access Data through, the ADHIE (such as clinical laboratories and pharmacies).

De-Identified Health Information/Data	Any Patient Health Information or Patient Data that is anonymized (i.e. does not identify a patient and with respect to which there is no reasonable basis to believe that the information can be used to identify a patient) in accordance with the requirements of Applicable Laws.
Disaster Relief Agency	A government agency with authority under UAE law to declare an Emergency Event or assist in locating individuals during an Emergency Event or a third-party contractor to which such a government agency delegates the task of assisting in the location of individuals in such circumstances and that has signed a Participant Agreement with ADHIE and accesses Data via the ADHIE Platform.
DOH	Department of Health (DOH) is the regulative body of the healthcare sector in the Emirate of Abu Dhabi.
Electronic System	Software, portal, platform or other electronic medium controlled by a Healthcare Professional and/or a Healthcare Facility, through which they Process or have the potential to Process the Patient Data.
Emergency Event	A circumstance in which a government agency declares a state of emergency or activates a local government agency incident command system or similar crisis response system.
Encounter	In relation to a patient, the period from when that Patient is first brought under the care of a Healthcare Professional at a Healthcare Facility until the time that Patient 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.
External Advisory Council	Major stakeholder groups from the healthcare industry in the Emirate of Abu Dhabi consulted by the ADHIE Operator from time to time to ensure appropriate engagement of industry experts.
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 Abu Dhabi 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 ADHIE's operations, infrastructure, and data management to ensure accountability and a protection of Abu Dhabi's public interest.
Health System Stakeholders	This includes Patients, Healthcare Facilities, Insurers, national and local health regulators, and other relevant entities.
Healthcare Facility	A DOH licensed establishment (including any hospital, clinic, surgery, pharmacy, diagnostic center, and other facility) where healthcare services are provided by Healthcare Professionals in the Emirate of Abu Dhabi.
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.).
Healthcare Professional	A healthcare professional who treats or deals with Patients in the Emirate of Abu Dhabi who is licensed & regulated by DOH
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; (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 it; (h) if that Participant ceases, or appears in the reasonable opinion of ADHIE 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.
Insured Person	Any individual who is insured for healthcare services in the Emirate of Abu Dhabi by a Payer.
Insured Person Patient Data	In relation to each Insured Person, Data relating to an Encounter with that Insured Person that is made available to the HIE Platform by each Healthcare Facility that provides healthcare services to that Insured Person from time to time in accordance with the requirements and timeframes of the Applicable Laws issued, brought into effect and maintained by DOH 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.
Interoperability	The interfacing of the ADHIE 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.
KPIs	The key performance indicators to be agreed and developed between the ADHIE Operator and the DOH.
Launch Schedule	Required onboarding date for Healthcare Facilities to the ADHIE Platform assigned by the ADHIE Operator.

Malicious Software	Any software, virus, Trojan horse, time bomb or other code (which can take the form of but not limited to Java applets, 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 ADHIE Platform or Patient Data or theft or damage to the ADHIE Platform or Patient Data or otherwise impairs the operation of the ADHIE Platform or the ability to Transact Patient Data.
Participant	An entity or person who enters into the Participant Agreement on behalf or one or more Healthcare Facilities, which authorises those Healthcare Facilities and their respective Healthcare Personnel to access, use or receive services via, or supply Data to, the ADHIE Platform.
Participant Agreement	The agreement made by and between the ADHIE Operator and each Participant, which sets forth the terms and conditions governing the operation of the ADHIE Platform and the rights and responsibilities of the Participants and the ADHIE with respect to the ADHIE 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 ADHIE 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 Patient Data and interface with the ADHIE Platform.
Participation Criteria	The criteria specified by ADHIE Operator from time to time, DoH Policies, the ADHIE Platform Interface Standards, the ADHIE Platform Access Requirements, Data Specifications and the Data Onboarding Requirements.
Parties	ADHIE Operator and each Participant, and 'Party' shall be construed accordingly.
Patient	A person who receives (or has received) healthcare services at a Healthcare Facility or otherwise from a Healthcare Professional from time to time.
Patient Data	In relation to each individual who receives healthcare services in the Emirate of Abu Dhabi, Data (including but not limited to medical records) relating to each Encounter with that individual that resides and is Processed on a Participant's System in accordance with the Participant Agreement and the Policies.

Patient Health Information ('PHI')	Any Patient Data, including any health and other information, text, radiological images, 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 patient the provision of health care to the Patient, or the payment for health care.
Personal Representatives	A person who manages the legal affairs of another because of incapacity or death.
Policies[1]	Refer to decisions, plans, and actions that are undertaken to achieve DOH's health care goals for Abu Dhabi. DOH'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.
Processing	Any operation or set of operations which is performed upon Patient Data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction and **Processed**, **Processes** and **Process** shall be construed accordingly
Research	The systematic investigation, including research development, testing and evaluation designated to develop or contribute to generalizable knowledge, including clinical trials.
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.
Sensitive Health Information	Special categories of health information as identified by ADHIE Operator that require additional restrictions on disclosure and use as determined by ADHIE Operator from time to time, which may include information regarding: a VIP Patient (which includes but is not limited to any VIP Patient Data); chemical dependency; HIV/AIDS status; mental health; alcohol and substance abuse; reproductive health; genetic testing information; and sexual health (including sexually transmitted diseases).

[1] DOH Healthcare Regulator Manual.

System Access	The ability or authority to interact with the ADHIE Platform; a means by which one may input or output data from the ADHIE Platform. Access requires authorization and proper clearance in accordance with Polices and the Participation Criteria.
Third Party	Each person or entity, which is not a Party to the Participant Agreement.
Transact	To send, supply, submit, route, make available to, upload, request, receive, respond to or publish Patient Data via the ADHIE Platform and 'Transacted' and 'Transaction' shall be construed accordingly.
VIP Patient	A Patient identified by the ADHIE Operator as a VIP who receives or has received healthcare services in the Emirate of Abu Dhabi and in respect of whom there are increased levels of control over access to that Patient's Data.
Workstation	An electronic computing device, for example, a lap or desk computer, or any other device that performs similar functions and electronic media stored in its immediate environment.

Executive Summary

The Department of Health of Abu Dhabi (DOH) is keen to promote the meaningful exchange of health information between Health System Stakeholders across the Emirate. The vehicle for this exchange is the Abu Dhabi Health Information Exchange (ADHIE), motivated by DOH's enduring commitment to ensure better access to care, to continually improve quality of care, and to safeguard the sustainability of health sector resources. The ADHIE initiative also supports many of DOH's strategic priorities, including the promotion of an integrated continuum of coordinated care and the promotion of integrated health informatics and eHealth.

To support such initiative, DOH has developed this policy, which lays the framework for developing the ADHIE and clarifies the roles and responsibilities of key Health System Stakeholders as they relate to participation, data management, and data quality. This overarching policy identifies the following priorities:

1. Universal stakeholder participation.
2. Universal patient participation.
3. Safe storage, transmission, and proper use of healthcare data.
4. Interoperability and high-quality data.

The health sector in Abu Dhabi needs clear direction to achieve these identified objectives. Thus, DOH seeks to provide a clear road map that sets out the roles and responsibilities of all the concerned stakeholders in the health sector so that it is prepared to face future challenges and continue to deliver world class healthcare.

1. Introduction

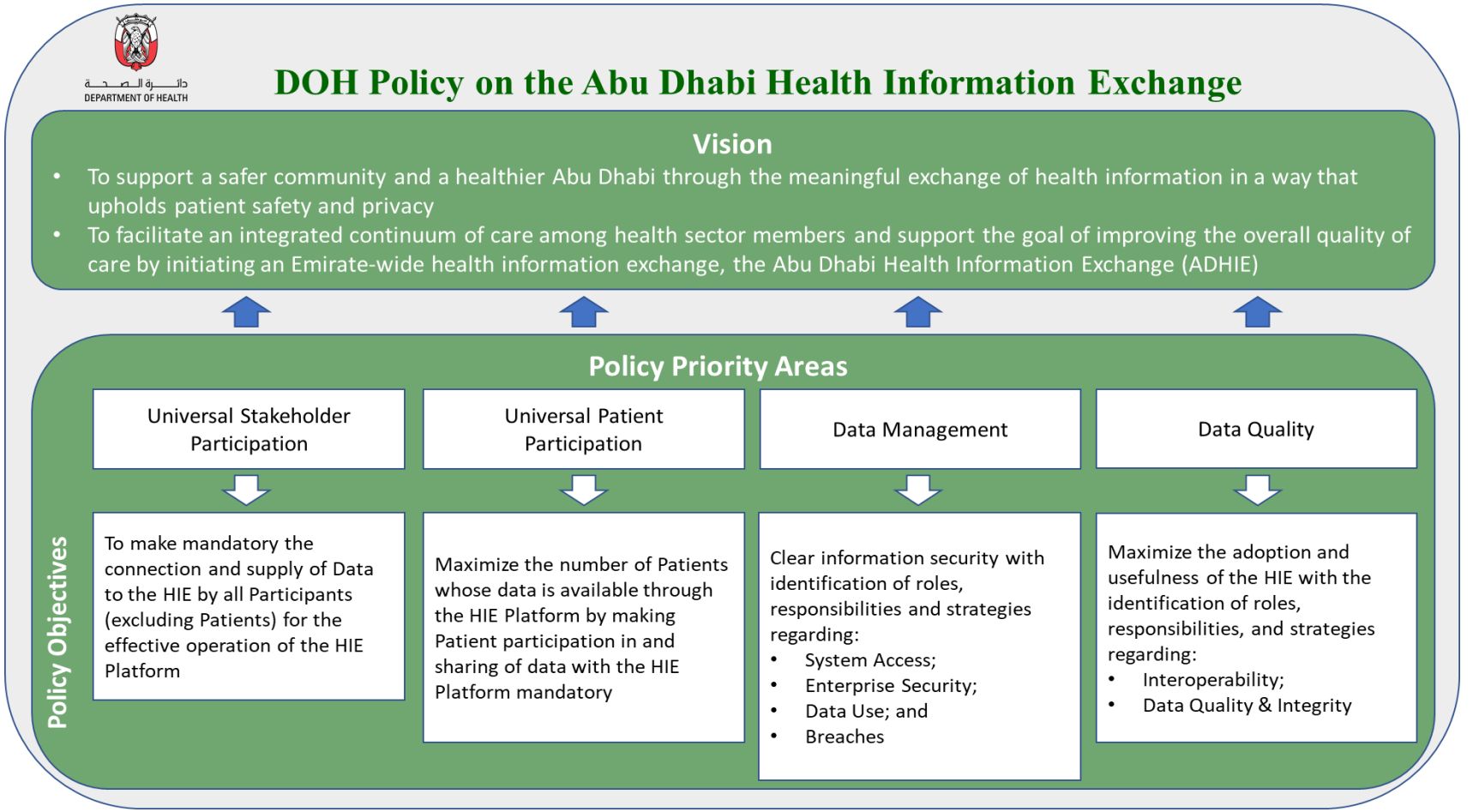
The Department of Health of Abu Dhabi (DOH) is committed to ensuring better access to health services, to continually improving quality of care, and to safeguarding the sustainability of sector resources. This commitment is all the more crucial in today's healthcare environment, where per capita healthcare costs are rising, healthcare resources are inefficiently and sometimes inappropriately used or over-utilized, and system resources are strained. At the same time, advances in technology afford new ways to collect and use crucial healthcare data that can be mobilized to improve care coordination, allocate healthcare resources more efficiently, and advance more effective public health initiatives.
In line with this strategic priority and in an effort to improve the health sector more broadly, DOH is embarking on an Emirate-wide initiative to promote the meaningful exchange of health information via a common information infrastructure, the Abu Dhabi Health Information Exchange (ADHIE). The ADHIE will be developed as part of a public-private partnership with the ADHIE Operator that includes Health System Stakeholders at all levels throughout the Emirate.
Notably, the ADHIE offers new possibilities for improving care that have never been feasible on such a scale before, and this initiative helps advance many of DOH's strategic priorities, including the promotion of health informatics and eHealth. By providing one repository for all of a patient's crucial health information, the ADHIE allows providers, pharmacies, labs, insurers, and government authorities to coordinate care more effectively. Similarly, shared information can also better inform caregivers and help them reduce unnecessary procedures while improving the quality of care they provide. Additionally, the availability of De-Identified Health Data that the ADHIE will allow has enormous implications for

launching new public health programs to monitor and improve the health of the entire Emirate.
Figure 1 below provides a visual overview of this policy, which is structured as follows:

- Section (2) provides the purpose of this overarching policy.
- Section (3) sets out the vision and goal of this policy. It also highlights its key guiding principles.
- Section (4) identifies the policy priority, objectives, and strategies to facilitate meaningful care coordination and Patient Data exchange among healthcare sector members and improve overall quality of care via the ADHIE.
- Section (5) provides the implementation arrangements for this policy. Section (6) identifies procedural roles and responsibilities.

Importantly, this document establishes the regulatory framework for the ADHIE. Additional policies, guidelines, and standards related to health information exchange in the Emirate may be defined in the future by DOH and the ADHIE that will build on, clarify, and/or modify the provisions established here, including various technical standards to be published by the ADHIE Operator.

Figure 1: Overview of the DOH Policy on the Abu Dhabi Health Information Exchange



2. Purpose of This Policy

The purpose of this policy is to:

- Articulate the Emirate's vision and goal for the ADHIE by setting out DOH's sector-wide objectives and strategies to ensure that all Health System Stakeholders can actively participate in and benefit from the meaningful and safe exchange of health information.

3. Vision, Goal and Guiding Principles

3.1 Vision

- To support a safer community and a healthier Abu Dhabi through the meaningful exchange of health information in a way that upholds patient safety and privacy.
- To facilitate an integrated continuum of care among health sector members and support the goal of improving the overall quality of care by initiating an Emirate-wide health information exchange, the Abu Dhabi Health Information Exchange (ADHIE).

3.2 Goal

To establish a health information exchange across the Emirate of Abu Dhabi.

3.3 Guiding Principles

The Guiding Principles to this policy are as follows:

3.3.1 Patient privacy and safety: it is the responsibility of all Health System Stakeholders to prioritize the privacy and safety of Patient Health Information.

3.3.2 Continuous improvement: meaningful health information exchange requires a commitment to continuous improvement of policy, programmes, practices, and service delivery at all levels of the government.

3.3.3 Technology-neutral: policies, standards, and guidelines should not prescribe specific technological solutions but rather outline visions and requirements of safe and meaningful health information exchange that will endure as technology changes.

3.3.4 Transparency through stakeholder engagement: the commitment and active participation of all relevant stakeholders is required to advance and coordinate DOH's effort to improve the exchange of health information.

3.3.5 Accountability: all Participants and their staff are accountable where failings and non-compliance have been identified.

3.3.6 Sectoral coordination: it is the responsibility of all Health System Stakeholders at all levels both local and federal to work jointly towards the meaningful exchange of health information.

3.3.7 Evidence-based and forward-looking strategy: implementation strategies of the policy shall be evidence-based, forward looking and take into account emerging global trends and local cultural and physical needs.

3.3.8 Context sensitive: while taking into account best practices and existing best models for health information exchange, the policy and implementation of the policy shall be driven by local and regional realities and priorities.

3.3.9 Partnership: insurers and providers (public and the private sector) shall be seen as strategic partners driving the development of this policy and its implementation.

3.3.10 Coordination, collaboration and communication: are critical components of effective health information exchange at all levels amongst stakeholders.

4. Policy Priority, Objectives and Strategies

4.1 Policy Priority 1: Universal Stakeholder Participation

DOH seeks to ensure that all licensed Healthcare Facilities in the Emirate of Abu Dhabi participate in the Abu Dhabi Health Information Exchange (ADHIE) in compliance with the Abu Dhabi Health Information and Cyber Security Standard (ADHICS).
Policy objectives 1. Universal Participation by all Healthcare Facilities as Data Suppliers to the ADHIE Platform.

Objective 1: DOH seeks to ensure all Healthcare Facilities connect and exchange data with the ADHIE as required by the ADHIE for the effective operation of the ADHIE Platform.
Strategy 1: Set out the requirements for Healthcare Facilities, DOH, and ADHIE to ensure that Patient Health Information is capable of being exchanged through the ADHIE Platform in such a way that it can be used meaningfully to aid the goal of improved care coordination and quality.

4.1.1 DOH shall:

4.1.1.1 Develop and oversee the implementation of further policies, standards, and guidelines related to ADHIE participation as necessary in accordance with Federal and Abu Dhabi Laws and other regulatory instruments.

4.1.1.2 Ensure compliance with this policy and all other policies, standards, and guidelines related to ADHIE participation.

4.1.1.3 Perform its role taking into account its agreement with the ADHIE Operator to design, develop, implement, maintain and operate an ADHIE Platform.

4.1.2 All Healthcare Facilities shall:

4.1.2.1. Enter into a Participant Agreement with the ADHIE Operator in accordance with the format provided by the ADHIE Operator, and at the time required by the ADHIE Operator.

4.1.2.2. Procure that any operating or parent or other group company engaged by ADHIE under a Participant Agreement in respect of any Healthcare Facilities provides the ADHIE Operator with a declaration or other written notification itemising all Healthcare Facilities for which that operating or parent company is responsible, in accordance with the format provided by the ADHIE Operator, and at the time required by the ADHIE Operator.

4.1.2.3 Comply with the ADHIE Platform Access Requirements and other Participation Criteria throughout the Policies and Participant Agreement to be considered by the ADHIE Operator for access.

4.1.2.4 Actively participate in meaningful health information exchange, once connected to the ADHIE, by:

4.1.2.4.1 Accurately recording required data in their medical records systems.

4.1.2.4.2 Ensuring that their medical record systems are ready for integration with ADHIE in as per the ADHIE Launch Schedule.

4.1.2.4.3 Implementing and supporting necessary infrastructure to connect to the ADHIE, including hardware and software interfaces and applications, at its own cost.

4.1.2.4.4 Complying with all relevant processes, protocols, and requirements of DOH, the ADHIE, and other relevant entities related to Health Information Exchange technology, privacy, security, and use.

4.1.2.4.5 Supplying and making available for access by the ADHIE Platform all Person Patient Data, in a way that accurately and comprehensively represents the Patient Data in their medical records system.

4.1.2.5 Ensure compliance of all systems and processes using ADHIE data with the Abu Dhabi Health Information and Cyber Security Standard (ADHICS) (as amended or replaced from time to time) and other relevant information security regulations.

4.1.3 ADHIE shall:

4.1.3.1 Support the development and implementation of policies, standards, and guidelines related to participation in the ADHIE in accordance with Federal and Abu Dhabi Laws and other regulatory instruments.

4.1.3.2 Establish and maintain ADHIE IT infrastructure, systems and processes.

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

4.1.3.4 Ensure compliance of all ADHIE systems and processes with the Abu Dhabi Health Information and Cyber Security Standard (ADHICS) and other relevant information security regulations.

4.2 Policy Priority 2: Universal Patient Participation

The DOH seeks to ensure that all licensed Healthcare Facilities in the Emirate of Abu Dhabi maximize the number of patients whose data is available through the ADHIE Platform.
Policy objectives 2. Universal participation by all patients to the ADHIE Platform

Objective 2: Maximize the number of patients whose data is available through the ADHIE Platform through making universal patient participation in and sharing of data with the ADHIE Platform mandatory.
Strategy 2: Set out the requirements for Healthcare Facilities and DOH to establish universal participation of patients in the ADHIE and to inform patients of their role in the ADHIE.

4.2.1 DOH shall:

4.2.1.1 Develop and oversee the implementation of further policies, standards, and guidelines related to ADHIE participation as necessary in accordance with Federal and Abu Dhabi Laws and other regulatory instruments.

4.2.1.2 Require Healthcare Facilities to obtain patient consent for the sharing of Patient Data via the ADHIE in accordance with all DOH's Policies. To the extent patient consent for the sharing of Patient Data via the ADHIE is unavailable for any reason (e.g. for legacy data), DOH in accordance with all Federal and Emirate laws and pursuant to its authority as the regulator of the Healthcare sector in the Emirate of Abu Dhabi, requires and authorizes Healthcare Facilities to share and receive such Patient Data (notwithstanding the unavailability of patient consent) through the ADHIE as set out in any instructions from DOH and as set out in this policy.

4.2.1.3 Ensure compliance with relevant Applicable Law, in particular this policy and Article 23 of the Implementing Regulation of the Abu Dhabi Law No. (23) of 2005 Concerning Health Insurance in the Emirate of Abu Dhabi, both of whom mandate the sharing of Patient Data by Healthcare Facilities in the Emirate of Abu Dhabi.

4.2.2 All Healthcare Facilities shall:

4.2.2.1 Comply with relevant DOH regulatory requirements regarding patient rights and responsibilities

4.2.2.2 Seek patient consent for the sharing of Patient Data via the ADHIE in accordance with all DOH's Policies, including by incorporating the following into their standard patient consent forms from the effective date of this policy:

4.2.2.2.1 Patients consent to the sharing of their Patient Data via the ADHIE whether it is newly-generated or past Patient Data.

4.2.2.2.2 Patients provide their consent to the sharing of their newly-generated or past Patient Data via the ADHIE to the Healthcare Facility (and its relevant treating Healthcare Professionals and its other Authorized Users) requesting the consent, plus every other Healthcare Facility (and their respective treating Healthcare Professionals and other authorized users) who will send or receive or who may have sent or received that patient's Patient Data via the ADHIE at any time.

4.2.2.3 Comply with DOH's mandate to share Patient Data to the extent patient consent is unavailable.

4.2.2.4 Inform patients appropriately that sharing relevant patient Health Information with the ADHIE is part of their treatment

4.2.3 ADHIE shall:

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

4.3 Policy Priority 3: Data Management

The DOH seeks to ensure that all parties associated with the HIE will have minimum data management related requirements in place for safe access, storage, transmission and proper use of healthcare data.
Policy objectives A comprehensive approach to ADHIE Data Management with clear identification of roles, responsibilities and strategies regarding: 1. System Access 2. Enterprise Security 3. Data Use 4. Breaches

Objective 3: Adherence of all parties associated with the ADHIE to a comprehensive approach to ADHIE System Access. The primary intent of this objective is to limit exchange of Patient Health Information to the minimum number of individuals necessary for accomplishing the intended purpose of the exchange, thereby allowing patients to have confidence in the privacy of their Patient Health Information as it shared among participants.

This objective for System Access is met through four sets of strategic requirements: authorization, authentication, access and patient engagement.

Strategy 3.1: Set out the authorization requirements for Healthcare Facilities, ADHIE, and DOH to ensure that the policy objective for System Access is achieved.

4.3.1 All Healthcare Facilities shall:

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

4.3.1.2 Ensure it has valid and enforceable written agreements with each of its Authorized Users.

4.3.1.3 Develop, maintain and implement relevant access control policies and procedures.

4.3.2 ADHIE shall:

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

4.3.2.2 Establish categories of Authorized Users and access levels in the Participation Criteria that will ensure that an end user can access protected resources only if they are permitted to do so.

4.3.2.3 Define in the Participation Criteria whether and what types of Sensitive Health Information is transacted in the ADHIE from time to time.

4.3.2.4 Define in the Participation Criteria the types of Patient Health Information, including Sensitive Health Information that each category of Authorized User may access and the purposes for which they may access it.

4.3.2.5 Define in the Participation Criteria the purposes for which Authorized Users in those access levels may access Patient Health Information via the ADHIE Platform.

4.3.2.6 Utilize role-based access standards to establish appropriate categories of Authorized Users and to define the purposes for which access may be granted and the types of information that may be accessed.

Strategy 3.2: Set out the authentication requirements for Healthcare Facilities, ADHIE and DOH to ensure that the policy objective for System Access is achieved.

4.3.3 DOH shall:

4.3.3.1 Issue guidance on identity authentication if and when required.

4.3.4 All Healthcare Facilities shall:

4.3.4.1 Implement initial identity-proofing procedures that require Authorized Users to provide identifying materials and information upon application for access to the ADHIE Platform.

4.3.5 ADHIE shall:

4.3.5.1 Assume full authority for granting access privileges based on the Healthcare Facilities' authentication of each of its approved users.

Strategy 3.3: Set out the access requirements for Healthcare Facilities, ADHIE and DOH to ensure that the policy objective for System Access is achieved.

4.3.6 All Healthcare Facilities shall:

4.3.6.1 Ensure that Authorized Users comply with passwords standard developed by the ADHIE for access to the ADHIE Platform.

4.3.6.2 Provide appropriate and adequate training to assure the following minimum requirements are met:

4.3.6.2.1 On-site training, web-based training, or comparable training tools so that Authorized Users are familiar with the operation of the ADHIE Platform and the Policies and procedures governing access to and use of information via the ADHIE Platform.

4.3.6.2.2 Ensure that each of its Authorized Users undergoes such training prior to being granted access to the ADHIE Platform.

4.3.6.2.3 Ensure that each of its Authorized Users signs a hard or electronic certification that he or she has received training and will comply with the relevant terms of the Participant Agreement.

4.3.6.2.4 Ensure that each of its Authorized User undergoes continuing and/or refresher training on an annual basis as a condition of maintaining

Authorized User status and the Healthcare Facility must keep hard copy or electronic records of such training.

4.3.7 ADHIE shall:

4.3.7.1 Establish an automated user management system that will follow standard user management practices and comply with relevant Abu Dhabi and Federal regulations.

4.3.7.2 Provide initial training to Healthcare Facilities as set out in the Participation Criteria.

Strategy 3.4: Set out patient engagement requirements for Healthcare Facilities, ADHIE and DOH to ensure that policy objective for System Access is achieved.

4.3.8 All Healthcare Facilities shall:

4.3.8.1 Educate Patients and/or their personal representatives with respect to the terms and conditions upon which their Patient Health Information may be shared with Authorized Users.

4.3.8.2 Enable patients and/or their personal representatives' access to their own data.

4.3.9 ADHIE shall:

4.3.9.1 Take industry standard measures to promote a safe and secure Health Information Exchange that provides Healthcare Facilities and patients access to patient health information.

4.3.9.2 Facilitate access to Patient Health Information in the ADHIE Platform, when operational, through the ADHIE Patient Portal.

4.3.9.3 Direct patients to the appropriate source Healthcare Facilities who can assist them to resolve any inquiry regarding the accuracy or integrity of their Patient Health Information.

Objective 4: Ensure that all Patient Health Information exchanged is protected by reasonable security safeguards against such risks of loss or unauthorized access, destruction, use, modification or disclosure.

Strategy 4: Set out the requirements for Healthcare Facilities, DOH and ADHIE Operator to establish and maintain the appropriate administrative, physical, and technical safeguards to ensure the privacy and security of Patient Health Information while exchanging the sharing of such information.

4.3.10 All Healthcare Facilities shall:

4.3.10.1 Ensure the confidentiality, Integrity and availability of all Patient Health Information it receives, maintains, or transmits.

4.3.10.2 Protect Patient Health Information against any reasonably anticipated threats or hazards to the security or Integrity of such information.

4.3.10.3 Protect Patient Health Information against any reasonably anticipated uses or disclosures of such information that are not permitted or required by Applicable Laws.

4.3.10.4 Implement policies and procedures for granting secured access through a Workstation, transaction, program, process or other mechanism.

4.3.10.5 Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program or process.

4.3.10.6 Implement procedures for timely termination of access to the ADHIE Platform when the employment of a workforce member ends or as required.

4.3.10.7 Implement and maintain physical and environmental security policies and procedures to:

4.3.10.7.1 Safeguard and limit unauthorized physical access to its Electronic Systems and the facilities in which they are housed, to prevent tampering and theft;

4.3.10.7.2 Restrict access to all sensitive systems in data centres

4.3.10.8 Implement policies and procedures that:

4.3.10.8.1 Allow workstation access to the ADHIE Platform to only those that have been granted access rights;

4.3.10.8.2 Specify the appropriate use and functions to be performed as part of use of the ADHIE Platform;

4.3.10.8.3 Implement physical safeguards for all Workstations that access the ADHIE Platform including restricting physical access to only Authorized Users when possible.

4.3.10.9 Implement security measures to guard against unauthorized access to all electronic Patient Health Information that is being transmitted over an electronic communications network.

4.3.10.10 Perform a Risk Assessment on individual network components and identify vulnerabilities requiring action.

4.3.10.11 Establish and monitor secure connections for transferring Patient Health Information between the Participants and the ADHIE Platform prior to any data exchanges.

4.3.10.12 Develop and maintain an awareness and training policy to assure the proper use and security of the ADHIE Platform.

4.3.10.13 Ensure that its training program covers at a minimum:

4.3.10.13.1 Authorized access requirements to the ADHIE Platform.

4.3.10.13.2 Acceptable and improper use.

4.3.10.13.3 Breaches and Breach notification procedures.

4.3.10.13.4 The Participant's sanction policy for non-compliance.

4.3.10.14 Provide privacy and security training to each Authorized User prior to granting him or her access to the ADHIE Platform and document all such training.

4.3.11 ADHIE shall:

4.3.11.1 Establish an automated user management system that will follow standard user management practices and comply with relevant Abu Dhabi and Federal regulations.

4.3.11.2 Take industry standard steps designed to help ensure that Authorized Users only are able to access information in the ADHIE Platform, for patients with whom they have an established medical relationship or as allowed in special conditions as defined by the ADHIE.

4.3.11.3 Employ appropriate controls for safeguarding patient and user information within the ADHIE Platform.

4.3.11.4 Regularly review and audit the ADHIE Platform to ensure proper use and security.

Objective 5: Adherence of all parties associated with the ADHIE to a comprehensive approach regarding the legitimate use, storage, processing, sharing and transfer of Data by and in relation to the ADHIE Platform and compliance with Applicable Laws relating to Data use.

Strategy 5: Set out requirements for Healthcare Facilities, DOH, and ADHIE to ensure appropriate and legitimate Data Use.

4.3.12 DOH shall:

4.3.12.1 Access Patient Data through an ADHIE Platform clinical viewer or portal for public health activities authorized by Applicable Laws. Examples of permissible uses of Patient Data include, but are not limited to:

4.3.12.1.1 To investigate suspected or confirmed cases of communicable disease.

4.3.12.1.2 To review, assess and analyse the vaccine coverage data per target population

4.3.12.1.3 Generate required vaccine certificate for both Healthcare Professionals and person (parents and guardians)

4.3.12.1.4 To ascertain sources of infection.

4.3.12.1.3 To conduct investigations to assist in reducing morbidity and mortality.

4.3.12.1.4 To investigate the causes of disease, epidemics, the sources of mortality, and the effect of localities, employments and other

conditions, upon the public health for scientific studies and Research which have for their purpose the reduction of morbidity and mortality and the improvement of the quality of medical care through the conduction of medical audits.

4.3.12.1.5 For infection reporting purposes.

4.3.12.1.6 For quality improvement and quality assurance activities.

4.3.12.1.7 For new-born disease screening, new-born hearing screening and early intervention.

4.3.12.1.8 For any other public health activities authorized by the Applicable Laws.

4.3.12.2 Permit the uploading of Patient Data from the records of a Data Supplier to ADHIE Platform, provided that the ADHIE does not make the information accessible to any party, except as otherwise outlined in this policy and/or the Participant Agreement or in any Applicable Laws.

4.3.12.3 Comply with all relevant Data Management and Data Quality requirements and responsibilities as set out in this policy

4.3.13 All Healthcare Facilities shall:

4.3.13.1 Use Patient Health Information received through the ADHIE Platform only for purposes permitted by Applicable Laws and this Policy.

4.3.13.2 Only use the ADHIE Platform for purposes that are strictly limited to clinical treatment, operations and uses as described in this policy and as outlined in the Participant Agreement and as may be specified by the ADHIE Operator from time to time.

4.3.13.2.1 Examples of permitted uses of Patient Data received via the ADHIE Platform include:

4.3.13.2.1.1 Patient identification upon presentation for medical treatment.

4.3.13.2.1.2 Patient record lookup associated with an Encounter (whether in-person or virtual).

4.3.13.2.1.3 Patient diagnosis, treatment, payment, and related Healthcare Operations, etc.

4.3.13.2.2 Examples of non-permitted uses of Patient Data received via the ADHIE Platform include but are not limited to:

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

4.3.13.2.2.2 A Healthcare Professional disclosing Patient 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.

4.3.13.2.2.3 Access or use of personally identifiable Patient Health Information by Healthcare Professionals who are not associated with the treatment of that specific Patient or cohort of Patients.

4.3.13.2.2.4 distribution to Third Parties.

4.3.13.2.2.5 granting access to Third Parties.

4.3.13.2.2.6 use for commercial gain or marketing purposes.

4.3.13.2.2.7 Use of Patient Data to form a health information exchange (other than the ADHIE Operator).

4.3.13.2.2.8 Sub-licensing of Patient Data.

4.3.13.2.2.9 Storage of patient data in a cloud environment

4.3.13.2.2.10 Transfer, transmit, share, make available or provide access to any Patient Data that is received or made available from or accessed through the ADHIE Platform outside the United Arab Emirates

4.3.13.2.2.11 Ingesting, storing, or recording any Patient Data that is received or made available from or accessed through the ADHIE Platform into its own system.

4.3.13.3 Take all necessary steps to protect against any misuses or disclosures of Patient Health Information.

4.3.13.4 Establish measures for ensuring the appropriate privacy and security controls are in place in order to protect the confidentiality, availability and Integrity of Patient Data that is being exchanged and made available on the ADHIE Platform. This includes the establishment of policies and procedures and other such controls to protect against any threats or hazards to the security or Integrity of such information.

4.3.13.5 Establish and comply with its own internal policies and procedures regarding disclosures of Patient Health Information and the conditions to be met and documentation to be obtained, if any, prior to making such disclosures.

4.3.13.6 Shall disclose through the ADHIE Platform only the minimum amount of Patient Health Information as is necessary as determined by ADHIE Operator.

4.3.13.7 Disclosures to a Healthcare Facility for treatment purposes and disclosures required by Applicable Laws are not subject to this provision of this policy.

4.3.13.8 Request only the minimum amount of Patient Health Information through the ADHIE Platform as is necessary for the intended purpose of the request. This provision of this policy does not apply to requests by Healthcare Facilities for treatment purposes.

4.3.13.9 Ensure that disclosure of information accessed through the ADHIE Platform is in compliance with the Policies and all Applicable Law.

4.3.14 ADHIE shall:

4.3.14.1 Disclose Patient Data to DOH for the purpose of public health reporting, including monitoring disease trends, conducting outbreak comparative effectiveness of medical treatments (including pharmaceuticals), conducting adverse drug event reporting, and informing new payment reforms.

4.3.14.2 Grant Organ Procurement Organization's access to the ADHIE Platform solely for the purpose of facilitating organ, eye or tissue donation and transplantation.

4.3.14.3 Access Patient Data via the ADHIE Platform to enable the ADHIE to perform system maintenance, testing and troubleshooting and to provide similar operational and technical support to participants and patients.

4.3.14.4 Comply with all relevant Data Management and Data Quality requirements and responsibilities as set out in this policy.

Objective 6: Minimize the risk of security breaches with the ADHIE Platform, its Data, infrastructure, and operations. Ensure secure storage and legitimate, compliant use of Data and address breach notification criteria and processes, mitigation processes and penalties.

Strategy 6: Set out the requirements and responsibilities when dealing with Breaches, which may include but are not limited to, instances involving the acquisition, access, use, or disclosure of Patient Health Information in a manner not permitted under this Policy and all Applicable Laws.

4.3.15 DOH shall:

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

4.3.15.2 Audit compliance with relevant policies and procedures.

4.3.15.3 Continuously improve related regulatory and compliance frameworks.

4.3.16 All Healthcare Facilities shall:

4.3.16.1 Obtain insurance coverage to indemnify the potential consequences of a breach to the extent set out in the Participation Criteria.

4.3.16.2 Develop and implement internal policies and procedures regarding Breaches which describe the different mechanisms for reacting to such Breaches based on the type of Breach (e.g. accidental disclosure, suffering

from a successful external attack, employee data misuse, etc.), and must include a notification process and a root cause analysis.

4.3.16.3 Train Authorized Users regarding breaches and breach notifications.

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

4.3.16.5 Notify patients affected, and any applicable regulatory agencies as required by and in accordance with Applicable Laws.

4.3.17 ADHIE shall:

4.3.17.1 Notify any Healthcare Facilities whose Patient Data was subject to the Breach, following ADHIE becoming aware of the details of such breach.

4.3.17.2 As deemed appropriate by ADHIE Operator, mitigate (or require the applicable participant to mitigate) to the extent practicable, any harmful effect of such Breach that is known to the ADHIE Operator or the Participant in respect of their respective areas of responsibility with regards to the ADHIE Platform. The ADHIE Operator's mitigation efforts shall correspond with and be dependent upon their internal risk analyses.

4.3.17.3 Require the Healthcare Facility to notify patients affected by the Breach and any applicable regulatory agencies as required by and in accordance with Applicable Laws. Affected individual(s) (in this case, a patient) must be notified of a Breach without undue delay but in no event later than 60 days from discovery.

4.3.17.4 Develop and implement internal policies and procedures regarding breaches, including processes for investigation of root cause

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

4.3.17.6 Notify the DOH of any breach as soon as reasonably practicable after determining that a Breach occurred, but in any event within 5 Business Days.

4.3.17.7 Investigate breach root causes and establish preventive plans and actions

4.3.18 A Breach excludes the following, as determined by the ADHIE Operator:

4.3.18.1 Any unintentional acquisition, access, disclosure, or use of Patient Health Information by a workforce member or person acting under the authority of the ADHIE or a Healthcare Facility, if such acquisition, access, or use was made in good faith, the root cause is remedied promptly, and within the scope of authority and does not result in further use or disclosure in a manner not permitted under Applicable Laws;

4.3.18.2 Any inadvertent disclosure by a person who is authorized to access Patient Health Information at the ADHIE or Participant to

another person authorized to access Patient Health Information at the ADHIE or participant, or organized health care arrangement in which a participant participates, and the information received because of such disclosure is not further used or disclosed in a manner not permitted under Applicable Laws; or

4.3.18.3 A disclosure of Patient Health Information where the ADHIE Operator or participant has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

4.4 Policy Priority 4: Data Quality

DOH seeks to ensure that all Patient Data that is shared with the ADHIE Platform is accurate, complete, relevant, and up-to-date to ensure its usefulness. All solutions and components that support ADHIE Platform interoperability, shall be based on open standards and not be dependent on any proprietary technologies.

Policy objectives
A comprehensive approach to ADHIE Data Quality with clear identification of roles, responsibilities, and strategies regarding:

1. Interoperability
2. Data Quality & Integrity

Objective 7: Achieve Interoperability of Data provided by Healthcare Facilities, such that the Data provided by one Healthcare Facility can meaningfully be used by another Healthcare Facility to improve the quality and coordination of care.

Strategy 7: Set out the requirements and standards for all solutions and components that support ADHIE Platform interoperability.

4.4.1 All Healthcare Facilities Shall:

4.4.1.1 Develop, implement and maintain an electronic interface between its Electronic System and the ADHIE Platform in accordance with the ADHIE Platform Interface Standards and the policies to enable the Transaction of Patient Data between that Participant and the other Participants.

4.4.1.2 Develop and implement an Interoperability Policy that is line with the Participation Criteria and this Policy.

4.4.1.3 Ensure that network connectivity from its own premises is in place to the ADHIE Platform data centres.

4.4.1.4 Ensure that its connection to and use of the ADHIE Platform does not include, and that any method of transmitting of Data (including any Patient Data) will not introduce, any program, routine, subroutine, or data (including Malicious Software or "malware," viruses, worms, and Trojan Horses) which will disrupt the proper operation of the ADHIE Platform or any part thereof or any hardware or software used by the ADHIE Operator in connection therewith, or which, upon the occurrence of a certain event, the passage of time, or the taking of or failure to take any action will cause the ADHIE Platform or any part thereof or any hardware, software or Data (including any Patient Data) used by the ADHIE Operator or any other Participant in connection therewith, to be destroyed, damaged, or rendered inoperable.

4.4.2 ADHIE Shall:

4.4.2.1 Establish interoperability standards and agreements that can be leveraged for all Healthcare Facilities.

4.4.2.1.1 This includes a section in the Participant Agreement that defines the roles and responsibilities of each party, monitoring the exchange of information with each Participant to ensure requirements are being met and take corrective action when the exchange of information does not follow the terms of the agreement.

4.4.2.2 Establish system interoperability standards that may include the following:

4.4.2.2.1 Domain Data Content and Structure Standards: includes information models, data naming standards, and controlled vocabularies. These represent semantic specifications that support business process level Interoperability.

4.4.2.2.2 Messaging and Transport Standards: covering message packaging, transport and network protocols. These may be considered more in the realm of syntactic standards that support technical interoperability. Examples include:

4.4.2.2.2.1 Private Network: Use of a private network service should be considered as part of a risk analysis, that transports all messaging through a private Wide Area Network (WAN)

4.4.2.2.2.2 SSL: Alternatively, secure data transport over the public Internet may utilize Secure Sockets Layer (SSL) protocol, the most widely adopted security protocol standard for the Internet.

4.4.2.2.2.3 'Web services' are the industry standard for platform neutral, distributed application Interoperation over the Internet. Web services should be used to effect data sharing across the ADHIE Platform.

Objective 8: Ensure the quality and integrity of patient Data provided by Healthcare Facilities.

Strategy 8: Set out the requirements and standards to ensure that all Patient Data shared with the ADHIE Platform is valid, accurate, complete, relevant, unique, consistent, and up-to-date.

4.4.3 All Healthcare Facilities Shall:

4.4.3.1 Be solely responsible for the quality of the Patient Data transacted.

4.4.3.2 Develop and implement applicable internal policies and procedures to ensure Data quality, including but not limited to the following:

4.4.3.2.1 Identification and standardization of data entry fields and processes for entering Data that is supplied to the ADHIE Platform.

4.4.3.2.2 Implementation of real-time quality checking, including the use of validation and feedback loops.

4.4.3.2.3 Use of Best Practices for the design, implementation and quality reviews of interface development to avoid errors.

4.4.3.2.4 Methods to receive patient feedback regarding erroneous information.

4.4.3.2.5 Procedures to correct erroneous information in order to ensure that incorrect information does not re-enter the system.

4.4.3.2.6 Notify the ADHIE Operator if, in response to a request by a patient, the Participant or Data Supplier makes any corrections to the Patient's erroneous information.

4.4.4 ADHIE Shall:

4.4.4.1 Direct patients to the appropriate participants who can assist them to resolve an inquiry or dispute over the accuracy or Integrity of their patient Health Information, and to have erroneous information corrected or to have a dispute documented if their request to revise data is denied.

4.4.4.2 Not be responsible for the content of any information transmitted or received through the ADHIE Platform or liability related to the accuracy, content, currency, completeness, content, or delivery of any Data on the ADHIE Platform.

5. Implementation Arrangements

5.1 Roles and Responsibilities

Objective 9: Engagement of Health System Stakeholders.

Strategy 9: Set out the roles and responsibilities for the DOH, Healthcare Facilities, and ADHIE Operator to fulfil their commitment towards the successful design, implementation, operation, adoption, and maintenance of the ADHIE Platform.

5.1.1 DOH shall:

5.1.1.1 Regulate the health system and ensure all regulatory provisions are enabled to address service gaps, inefficiencies, malpractice, or unfairness.

5.1.1.2 Have in place governance measures to ensure the safety of patients and Patient information related to health information exchange.

5.1.1.3 Provide the necessary stewardship, ensure that the requirements set out in this Policy are met through its regulatory powers and where necessary, set out further regulatory measures to address the current and future health system needs for health information exchange.

5.1.2 All Healthcare Facilities shall:

5.1.2.1 Meet the requirements as set out by the DOH and ADHIE Operator to ensure the safety and privacy of Patient Data and the meaningful exchange of healthcare information.

5.1.2.2 Be responsible and accountable for the effective and appropriate use and safeguarding of Patient Health Information and for compliance with DOH directions set out in this Policy and other relevant UAE rules and regulations.

5.1.3 ADHIE shall:

5.1.3.1 Establish Governance arrangements, which include DOH and Healthcare Facility market representation, that oversee the implementation of the ADHIE regulatory framework and provide strategic support to enable the ADHIE to achieve its operational objectives.

5.1.3.2 Receive, access, use and Process Patient Health Information for the purpose of developing, implementing, managing, supporting and maintaining the ADHIE Platform and integrating the ADHIE Platform and meet the requirements as set out by the DOH and this Policy

5.2 Escalation and Enforcement

Objective 10: Ensure escalation and enforcement of the ADHIE policy priority as outlined in this Policy.

Strategy 10: Set out DOH approach for escalation and enforcement to ensure compliance with this Policy.

5.2.1 DOH shall:

5.2.1.1 Escalate and take all appropriate actions where it determines that non-compliance has occurred.

5.2.1.2 Exercise its powers in a flexible manner to ensure that regulatory action is targeted where it is needed.

5.2.1.3 Bring to an end any failure to comply with this Policy.

5.2.1.4 Prevent any such failure from being repeated in the future.

5.2.1.5 Administer its investigative process in order to determine any non-compliance.

5.2.1.6 Utilize escalation procedures where non-compliance has occurred. Once DOH has undertaken its investigation appropriate enforcement will be subject to DOH's determination of the level of breach or non-compliance and may include the following measures with specified timescales for compliance and/or action:

5.2.1.6.1 Provide advice

5.2.1.6.2 Set out a remedial action plan

5.2.1.6.3 Refer the matter to the Competent Committee with a view to:

5.2.1.6.4 Issue a reprimand, notice or warning

5.2.1.6.5 Issue notice of suspension

5.2.1.6.6 Withdrawal of licensure

5.2.1.6.7 Recommend legal proceedings

5.2.1.6.8 Any other appropriate action

5.2.1.7 Suspend or withdraw a Healthcare Facility's license if they fail to comply with the ADHIE Launch Schedule .

5.2.1.8 Administer fines or penalties, including fines for Healthcare Professionals and other users of the ADHIE Platform, pursuant to Applicable Laws.

5.2.1.9 Administer financial incentives, including amendments to the reimbursement rates, pursuant to Applicable Laws.

5.2.2 ADHIE Shall:

5.2.2.1 Have the right to immediately suspend or terminate a Participant's right to Transact Patient Data, interface with the ADHIE Platform and access or use the ADHIE Platform if entitled to do so under the Participant Agreement and/or if any one or more of the following occurs:

5.2.2.1.1 the Participant breaches or no longer satisfies the Participation Criteria for any reason;

5.2.2.1.2 the Participant no longer is a holder of any licence, consent, permit, authorisation, clearance or other approval necessary to enable the Healthcare Facility to operate as a Healthcare Facility in the Emirate of Abu Dhabi or no longer has any medical malpractice insurance or other insurance Policies required by Applicable Law;

5.2.2.1.3 the Participant commits a material breach of any of its obligations under this Policy or the Participant Agreement which is incapable of remedy, or which is capable of remedy but fails to remedy it or persists in such breach after 30 days of having been required in writing to remedy or desist;

5.2.2.1.4 the Participant is not in compliance with any Applicable Laws or if the ADHIE Operator is aware or reasonably believes any development may have a material impact on the Participant's ability to perform its obligations under this Participant Agreement effectively and in accordance with Applicable Laws;

5.2.2.1.5 the Participant is subject to an Insolvency event. Each Participant shall notify the ADHIE Operator if it experiences any Insolvency Event.

5.2.2.1.6 the relevant Participant breaches, or the ADHIE Operator reasonably suspects the relevant Participant is in breach of this Policy or any related Applicable Laws

5.2.2.1.7 ADHIE Operator is instructed to suspend or terminate the Participant's right to Transact Patient Data, interface with the ADHIE Platform and access or use the ADHIE Platform by the DOH; and/or

5.2.2.1.8 the relevant Participant undergoes a Change of Control not previously approved in writing by the ADHIE Operator. Each Participant shall notify the ADHIE Operator if it experiences any Change of Control.

5.3 Monitoring and Evaluation

Objective 11: The DOH, ADHIE Operator, and Healthcare Facilities to monitor and continuously improve the performance of the ADHIE.

Strategy 11: Set out approach for the monitoring and evaluation of the ADHIE performance.

5.3.1 DOH shall:

5.3.1.1 Perform periodic audits, or their appointed third-party vendor, of Healthcare Facilities to ensure compliance with all Applicable Laws and Policies.

5.3.2 Healthcare Facilities shall:

5.3.2.1 Grant, and shall ensure that each of its subcontractors and Affiliates grant, to the ADHIE Operator and to its Authorized agents and DOH, a right of access to relevant Authorized Users and Participant Personnel, the Participant's systems and records and any other information as ADHIE Operator, its agents and DOH reasonably consider necessary to verify the Participant's compliance with this policy, the Participant Agreement, and other relevant DOH Policies.

5.3.2.2 Review periodic performance reports generated and prepared by ADHIE Operator.

5.3.2.3 Comply with the terms and requirements of this policy. DOH may impose sanctions in relation to any breach of requirements under this policy in accordance with the Complaints, Investigations, Regulatory Action and Sanctions Policy, Chapter IX, Healthcare Regulator Manual.

5.3.2.4 Report to DOH and ADHIE Operator any Breaches arising from the implementation or use of the ADHIE Platform that could potentially affect the security of Patient Health Information.

5.3.3 ADHIE shall:

5.3.3.1 Monitor the overall performance of the ADHIE through KPIs, which will be developed according to the process set out in the public-private partnership.

5.3.3.2 Act to remedy any underperforming KPI as defined by the Government Oversight and Policy Task Force.

5.3.3.3 Prepare periodic performance reports for Healthcare Facilities.

5.3.3.4 Report to DOH any Breaches arising from the implementation or use of the ADHIE Platform that could potentially affect the security of Patient Health Information.

6. Appendix

6.1 Procedural Roles and Responsibilities

6.1.1 DOH shall:

6.1.1.1 Notify immediately the ADHIE Operator in instances where an Authorized Users access rights should be terminated or blocked. [P3]

6.1.1.2 Notify the ADHIE of any Breach as soon as reasonably practicable after determining that a Breach occurred, but in any event within five Business Days. [P3]

6.1.2 Healthcare Facilities shall:

6.1.2.1 Pursuant to the Healthcare Facility's licensing agreement with the DOH, the Healthcare Facility is contractually obligated to adhere to the policies established by the ADHIE Operator. [P1]

6.1.2.2 Engage in legal agreements with the ADHIE Operator and other relevant entities that are necessary to secure patient privacy, data security, and the meaningful exchange of Patient Health Information. [P1]

6.1.2.3 Complete the readiness assessment and develop, implement, and maintain a Participant System in accordance with ADHIE Platform Interface Standards. [P1]

6.1.2.4 Adhere to the ADHIE Launch Schedule [P1]

6.1.2.5 Actively participate in meaningful health information exchange, once connected to the ADHIE, by:

6.1.2.5.1 Submitting required Patient Data in a timely manner to the ADHIE in accordance with the Participation Criteria. [P1]

6.1.2.5.2 Receiving required incoming Data from the ADHIE and integrating it into their own Participant Systems in a timely manner in accordance with the Participation Criteria. [P1]

6.1.2.5.3 Maintaining availability of their interface for the exchange of Patient Data in accordance with the Participation Criteria. [P1]

6.1.2.6 Implement the necessary internal policies and procedures to Prohibit Authorized Users from making available or supplying VIP Patient Data to the ADHIE Platform in accordance with the Participation Criteria. [P1]

6.1.2.7 Appoint Authorized Users and assign them to the appropriate Access Levels.

6.1.2.8 Provide the ADHIE Operator with a list of Authorized Users in a medium and format approved by the ADHIE Operator. [P3]

6.1.2.9 Provide notification to the ADHIE Operator in the manner required by ADHIE Operator whenever an Authorized User is added or removed by reason of termination of employment or otherwise and ensure notification of such change is given within 48 hours. [P3]

6.1.2.10 Ensure it has valid and enforceable written agreements with each of its Authorized Users that comply with ADHIE requirements from time to time, including by requiring the Authorized User to, at a minimum:

6.1.2.10.1 Comply with all Applicable Laws [P3];

6.1.2.10.2 cooperate with the Participant on issues related to the Participant Agreement [P3];

6.1.2.10.3 Transact Patient Data only for a Permitted Purpose [P3];

6.1.2.10.4 Use Patient Data received from another Participant or Authorized User in accordance with the terms and conditions of the Participant Agreement [P3];

6.1.2.10.5 As soon as reasonably practicable after determining that a Breach occurred, report such Breach to the Participant (but in any event within five business days [P3]; and

6.1.2.10.6 Refrain from disclosing to any other person any passwords or other security measures issued to the Authorized User by the Participant. [P3]

6.1.2.11 Establish and maintain a Master Patient Index that will provide single source of identification information for all participating systems. [P3]

6.1.2.12 Require its Authorized Users to sign a statement that they understand their obligations contained in this Policy and Participant Agreement. [P3]

6.1.2.13 Provide Authorized Users a written statement of their access rights. [P3]

6.1.2.14 Ensure that all Authorized Users are uniquely identified through the verification of the Emirates ID card of each Authorized User and keep a copy on file. [P3]

6.1.2.15 Ensure that each Authorized User can only access the ADHIE platform by means of a unique password and that each Authorized User is bound not to share that password with any other person. [P3]

6.1.2.16 Ensure that each Authorized User is assigned a unique user name and password to provide such Authorized User with access to the ADHIE Platform. [P3]

6.1.2.17 Comply with the following minimum password standards:

6.1.2.17.1 User ID must be unique. [P3]

6.1.2.17.2 Passwords must be at least eight characters long. [P3]

6.1.2.17.3 Passwords must be composed of at least three of the following: English uppercase letters, English lowercase letters, numeric characters, and special characters. [P3]

6.1.2.17.4 Password lifetime will not exceed 60 days. [P3]

6.1.2.17.5 Authorized Users cannot use the previous six passwords. [P3]

6.1.2.17.6 Shared or generic User ID's are not permitted. [P3]

6.1.2.17.7 Group or temporary user names shall be prohibited. [P3]

6.1.2.17.8 Authorized Users shall be prohibited from sharing their user names, passwords or other authentication tools (e.g., tokens), with others and from using the user names, passwords or other authentication tools of others. [P3]

6.1.2.18 Enforce a limit of consecutive failed access attempts because of incorrect username and password combinations by an Authorized User. After which access to the ADHIE Platform is disabled either by locking the account until release by the ADHIE or by locking the account for a specific period as specified by the

ADHIE, after which the Authorized User may re-establish access using appropriate identification and authentication procedures. If Authorized Users obtain or are granted access to the ADHIE Platform by way of Single Sign-on technology through a Participant's Participant System, the ADHIE may delegate the responsibility for enforcing this failed access attempt limitation to the Participant. [P3]

6.1.2.19 Ensure that an Authorized User is automatically logged out of the ADHIE Platform after a period of inactivity by such Authorized User. The termination shall remain in effect until the Authorized User re-establishes access using appropriate identification and authentication procedures. [P3]

6.1.2.20 Assign a unique name and/or number to all Authorized Users of the ADHIE Platform for identifying and tracking user identity. [P3]

6.1.2.21 Restrict access to all sensitive systems in data centres by using physical cages

on all servers to prohibit access to external ports and by disabling/removing the ability to insert, read or write to such devices. [P3]

6.1.2.22 Control and validate a person's access to facilities based on their role or function, including visitor control and access to software programs for testing and revision. [P3]

6.1.2.23 Implement policies and procedures that:

6.1.2.23.1 Terminate an electronic session after a predetermined time of inactivity. [P3]

6.1.2.23.2 Inhibit the use of removal media, ensure use of encryption technologies when deemed necessary. [P3]

6.1.2.23.3 Employ anti-malware protections mechanisms and assure they are up-to-date. [P3]

6.1.2.24 Not suspend or terminate their participation, their Transaction of Patient Data, or their interface with the ADHIE Platform without the prior written consent of the ADHIE Operator. [E&E]

6.1.2.25 Notify the ADHIE Operator as soon as possible after it becomes aware of any development that may have a material impact on its ability to perform its obligations in this Policy, the Participant Agreement, and any Applicable Laws. [E&E]

6.1.2.26 Discipline and sanction appropriately any of its respective Authorized Users who fail to act in accordance with this Policy, the Participant Agreement or in accordance with the Participant's related Policies and procedures, as well as all Applicable Laws. [E&E]

6.1.2.27 Notify the ADHIE and the DOH of any breach as soon as reasonably practicable after determining that a Breach occurred, but in any event within 5 working days. [P3]

6.1.2.28 Ensure that all internal policies and procedures that Healthcare Facilities are required to put in place or update as a result of this policy shall be in accordance with the Participation Criteria.

6.1.3 ADHIE shall:

6.1.3.1 Issue, manage and from time to time update, the Launch Schedule to Healthcare Facilities informing them when they are required to join the ADHIE. [P1]

6.1.3.2 Develop and disseminate a readiness assessment tool to be completed by the Healthcare Facility. [P1]

6.1.3.3 Establish mandatory Participation Criteria and other technical standards required by the Participant Agreement or for proper management of the ADHIE Platform, for Healthcare Facilities to comply with. [P1]

6.1.3.4 Inform health sector members when they are required to join the ADHIE; advanced notice of this participation requirement shall be given so that health sector members have a reasonable amount of time to on board. [P1]

6.1.3.5 Impose suitable measures on Healthcare Facilities in order to prevent VIP Patient Data from being exchanged or stored on the ADHIE Platform or made accessible to Authorized Users. [P1]

6.1.3.6 Establish and enter into a Participant Agreement with Healthcare Facilities in a format determined by ADHIE. [P1]

6.1.3.7 Remove or block access rights of Authorized Users within twenty-four (24) hours of notification for removal by the DOH or a Healthcare Facility. [P3]

6.1.3.8 Remove or disable Authorized Users accounts that have been inactive for a period of sixty (60) days or more. [P3]

6.1.3.9 Ensure that Authorized Users obtain access to the ADHIE Platform by use of a unique username and password. [P3]

6.1.3.10 As an added security precaution, all servers which contain patient and user information, must meet or exceed industry standards for server hardening, to prevent unauthorized disclosure or loss of Patient Data. [P3]

6.1.3.11 Implement operating procedures and the applicable controls based on industry standards that address:

6.1.3.11.1 Minimum security configurations and hardening measures [P3];

6.1.3.11.2 Malware protection [P3];

6.1.3.11.3 Ongoing patching [P3];

6.1.3.11.4 Capacity management [P3];

6.1.3.11.5 Audit Logging [P3]; and

6.1.3.11.6 Data backup. [P3]

6.1.3.12 Log all transactions of clinical data involving the ADHIE Platform to support periodic auditing. [P3]

6.1.3.13 Assure that log files cannot be altered, so that once written, they cannot be edited or deleted (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. [P3]

6.1.3.14 Identify criteria and requirements to segregate Patient Health Data groups to a separate logical network. This network must be protected by a firewall that

controls access and information flow only to use and function of the ADHIE Platform. The firewall must be configured to block unauthorized traffic and access as defined in the System Access Policy. Other technologies including the use of a private network, IP switching, Virtual Private Network (VPN) and multifactor authentication should also be considered as part of the overall level of trust and Risk Assessment. [P3]

6.1.3.15 Regularly review and audit the ADHIE Platform to ensure proper use and security. At a minimum, specific audit functions must include:

6.1.3.15.1 Review of system administrator authorizations and activity [P3].

6.1.3.15.2 Review of network intrusion detection system activity logs [P3].

6.1.3.15.3 Review of physical access to data centres [P3].

6.1.3.15.4 Procedures for follow-up on suspicious activity, such as indications of possible privacy or security breaches [P3].

6.1.3.15.5 Other review of technical, physical, and administrative safeguards as established by the Policies of the organization [P3].

6.1.3.16 Grant a Disaster Relief Agency access to the ADHIE Platform for the following information during an Emergency Event:

6.1.3.16.1 Patient name and demographics information. [P3]

6.1.3.16.2 Name of the Healthcare Facility from which the Patient received care during the Emergency Event, dates of Patient admission and/or discharge. [P3]

6.1.3.16.3 Access to information under this section may begin when the Emergency Event begins and shall cease when the Emergency Event ceases. [P3]

6.1.3.16.4 Information accessed under this section shall not reveal the nature of the medical care received by the Patient who is the subject of the access request unless otherwise permitted by Applicable Law or if the relevant government body, through executive order, temporarily suspends health information confidentiality laws that would otherwise prohibit such disclosure. [P3]

6.1.3.17 As it deems appropriate from time to time, establish procedures for auditing of additional functions, for example:

6.1.3.17.1 Review of network intrusion detection system activity logs. [P3]

6.1.3.17.2 Review of system administrator authorizations and activity. [P3]

6.1.3.17.3 Review of physical access to data centers. [P3]

6.1.3.17.4 Other reviews of technical, physical, and administrative safeguards as established by the Policies of the organization and industry standards. [P3]

6.1.3.18 Establish system interoperability standards that may include the following:

6.1.3.18.1 Domain Data Content and Structure Standards: includes information models, data naming standards, and controlled vocabularies. These represent semantic specifications that support business process level Interoperability. Examples include:

6.1.3.18.1.1 HL7 (version 2.x or 3.0) and NCPDP SCRIPT, the de facto industry messaging standards for general healthcare and prescription data respectively, should be used where applicable. The HL7 Reference Information Model offers a ready set of data standards that provide the semantic interoperability underpinning for HL7 messaging standards. [P3]

6.1.3.18.1.2 Clinical Terminology (SNOMED) for support a common computerized language for use across all provider organizations. [P3]

6.1.3.18.1.3 XML 1.0 is the data message notation standard for inter-application data communication and shall be the default message serialization format. [P3]

6.1.4 Emergency access to Patient Data on the ADHIE Platform is permitted when treating a patient with a qualified condition by (i) a Healthcare Professional; (ii) an Authorized

User acting under the direction of a Healthcare Professional; or (iii) an Advanced Emergency Medical Technician. These individuals may "break the seal" if the following conditions are met:

6.1.4.1 Treatment may be provided to the Patient, in the Healthcare Professional's or Advanced Emergency Medical Technician's judgment if a qualified condition exists and the patient is in immediate need of medical attention. [P3]

6.1.4.2 The Healthcare Professional or Advanced Emergency Medical Technician determines, in his or her reasonable judgment, that information that may be held by or accessible via the ADHIE Platform may be material to emergency treatment. [P3]

6.1.4.3 If an Authorized User acting under the direction of a Healthcare Professional "breaks the seal", such Authorized User must record the name of the Healthcare Professional providing such direction. [P3]

6.1.4.4 The Healthcare Professional, Advanced Emergency Medical Technician or Authorized User acting under the direction of a Healthcare Professional attests that all the foregoing conditions have been satisfied, and the ADHIE Platform software maintains a record of this access. [P3]

6.1.4.5 All Healthcare Facilities are required to track and document all "break the seal" occurrences and to assure conditions as described in the policy have been met.

6.1.4.6 The ADHIE Operator and/or DOH reserves the right to perform ongoing audits of all "break the seal" occurrences. [P3]

6.1.4.7 All Healthcare Facilities ensure that access to Patient Health Information via the ADHIE Platform utilizing "Break the Seal" when treating a patient terminates upon the completion of the emergency treatment. [P3]