



Riayati Program

Healthcare data confidentiality and privacy Policy

Document ID : RYT-PGM-POL-003

Date: 11 June 2020





Document History

Version No.	Date Change Approved	Description of Changes	Impacted Supporting Document(s)	Supporting Document Change / Version No.	Authors
1.0	NA	Initial Document	NA	NA	MOHAP

Table 1 Document Version History

Document Reviewer(s)	Signature	Date
MOHAP		11 June 2020

Table 2 Document Review Grid

Document Approver(s)	Signature	Date
MOHAP		11 June 2020

Table 3 Document Approver Grid

After the approvers accept this document, the approved version becomes the baseline. All changes to the baseline version will need to be approved by approvers mentioned above.



Table of Contents

1	Definitions	4
2	Introduction	6
3	Intended Audience	6
4	Data Confidentiality Policy	7
4.1	Consent to upload Healthcare Data to Riyati HIE	7
4.2	Patient Consent to view EHR by caregivers	7
4.3	Break-the-Glass Access for Emergency Care	8
4.4	Access sensitive Information	9
4.5	VIP Patient Data access	10
4.6	Access for Healthcare Analytics and reporting	10
4.7	Data De-identification and access for research purposes	11
4.8	User Authorization and Access Control	12
4.9	Audit Logs and Auditing Process	12
4.10	Protected Health Information (PHI) Breach Notification	13
4.11	Notification Services.....	13

Table of Tables

No table of figures entries found.



1 Definitions

MOHAP means Ministry of Health and Prevention, UAE

Riayati HIE means the Riayati Health Information Exchange a platform implemented and maintained by MOHAP for access to electronic medical record across the hospitals in Northern Emirates.

Provider Organization / Healthcare Facility means any entity (such as a hospital, nursing home, polyclinic, clinic, Daycare center, diagnostic center) licensed to provide healthcare services under the jurisdiction of MOHAP, UAE.

Healthcare Professional means a Healthcare professional having a valid practicing license from licensing authority of MoHAP, UAE and (i) employed by a Provider Organization to provide health care services to the patients; (ii) an Independent Healthcare professional providing services to the patients in individual capacity.

Patient means an individual whose Electronic Health Records (EHR) are stored in and are accessible through Riayati Health Information Exchange.

Participation Agreement means the agreement made between MOHAP and the Provider Organization intending to participate and get connected to the Riayati HIE. This agreement outlines the roles and responsibilities for the participating Provider Organizations and MOHAP and also sets forth the terms and conditions governing access to Riayati HIE.

Participating Healthcare organization also referred as healthcare facility means a Healthcare facility/Provider Organization (such as a hospital, nursing home, polyclinic, clinic, Daycare surgery, diagnostic center or any other healthcare Entity) that has entered into a Participation Agreement with MOHAP to exchange Electronic Health Records using Riayati HIE.

Sensitive Health Information means any information related to patient, for which special privacy protection is applicable under MOHAP or UAE regulations, including mental health, substance abuse, HIV/AIDS, reproductive health, sexually transmitted disease.

Consent Form means a consent form approved by MOHAP under which a patient has either given Consent or denied consent allowing access to his/her Electronic Health Information in a Break the Glass situation or as otherwise provided by these Policies.

Electronic Health Record (EHR) is a digital version of a patient's health information which includes but not limited to symptoms, allergies, complaints, diagnosis, clinician's notes, medical histories, treatment plan, diagnostic results, diagnostic images etc.

Protected Health Information (PHI) means individually identifiable health information. This includes the patient demographics, patient's health care record that is created or collected by a participating healthcare organization that can be linked to a specific individual.

VIP Patient A patient marked as a VIP in the Clinical Application for whom the data sharing and access controls will be different and more stringent as compared to the controls applicable for a general patient.

Riayati Provider Portal means the portal for the healthcare providers(doctors) to access electronic health information stored in the Riayati HIE.



Demographic Information means a patient's name, gender, address, date of birth, Emirates ID number, passport Number, Driving License Number and other personally identifiable information. This does not include any information regarding a patient's health or medical treatment

De-Identified Data is the Electronic Health information of an individual or a population for which there is no demographic information attached to relate the data to an individual

Emergency Event means a situation in which a Healthcare authority or government agency initiates crisis response activities to manage healthcare rendered in the UAE

Personal Representative means a person who is authorized as per the UAE law to consent to the disclosure of a patient's Electronic Health Information available in Riayati HIE.

Authorized User means an individual who has been authorized by a Participating Healthcare Organization to access information using Riayati Health Information Exchange, based on the user role, and Riayati policies and procedures.

Break-the-Glass means accessing a patient's Electronic Health Information without obtaining a Consent from patient in compliance with the Riayati policies and procedures.



2 Introduction

Ministry of Health and Prevention initiated the Riayati HIE program to transform the healthcare landscape by connecting to the digital health solutions that leverage clinical data to foster key structural changes and align goals and incentives to new, innovative delivery models of care. These actions primarily aim to improve the wellness of the population.

The Riayati journey began in 2015, when His Highness Sheikh Mohammed bin Rashid Al Maktoum announced the initiative to establish a national unified medical record system of patients in the UAE, in order to facilitate the movement of patients among healthcare providers, as well as to connect public hospitals and clinics. This is necessary to have up-to-date medical records in order to improve healthcare services provided in the UAE. Riayati will streamline efforts in the healthcare sector to build a modern and safe healthcare system with improved level of patient care and clinical outcomes.

Riayati Health Information Exchange will make quality healthcare data available for improvement of the patient care and support the futuristic innovative services like Clinical Decision Support, UAE specific clinical pathways, advanced analytics and Artificial Intelligence. . The Riayati program, will be the foundation for building a modern, sustainable and integrated health system that ensures patient's safety, provides quality care and population wellness.

This document sets the guideline for confidentiality of the healthcare data and patient privacy. This will be applicable for participating healthcare organizations and Healthcare Professionals to connect, share and access patient electronic health information using Riayati HIE

In addition to this document MOHAP and Riayati may publish additional policy documents, technical documents, amendments or annexures as deemed necessary from time to time.

3 Intended Audience

This document is applicable to the healthcare organization that has directly or indirectly entered into a Participation Agreement with Riayati HIE to submit and access Electronic Health Records, such as:

- MOHAP Hospitals and PHCs
- Private Hospitals
- Pharmacies
- Clinics and Polyclinics (Medical Centers)
- Diagnostic Centers
- Allied healthcare organizations

This document is also applicable to all healthcare IT solution providers, system integrators and vendors required to or intending to connect to the Riayati HIE either directly or through healthcare providers in Northern Emirates



4 Data Confidentiality Policy

Data Confidentiality policy sets the boundaries within which patient's Electronic Health Record can be accessed by the healthcare professionals working with Healthcare Organizations or as Individual care providers or shared across neighboring HIE network. This policy is patient centric, and the care providers and organizations are required to maintain certain degree of confidentiality as defined later in this document.

Riyati HIE puts patients at the center and empowers them with the right of confidentiality. Patient consent policy provisions that the patients can make informed decision about who can access their medical records and the choice is properly recorded and maintained in the Riyati HIE. The information related to the consent opted by the patient is not used for discriminatory purposes or as a condition for receiving medical treatment. It allows patients to create, modify, and revoke their consent at any time through Patient Portal published by MoHAP.

4.1 Consent to upload Healthcare Data to Riyati HIE

As per Riyati policy all the healthcare facilities connected to Riyati health information Exchange need to upload patient electronic health records to the Riyati HIE. The health records shall be uploaded digitally, as per the interoperability standards published by Riyati. No explicit patient consent is required to be taken by the healthcare facilities to upload patient electronic health records to the Riyati HIE.

The data uploaded to HIE will be viewed by the caregiver based on the patient consent as described in section 4.2 of this document

The data will be also used for healthcare planning, disease surveillance, statistical analysis and research purposes. No explicit patient consent is required for access to the data by the regulatory authorities for planning, disease surveillance, statistical analysis and research purposes.

4.2 Patient Consent to view EHR by caregivers

Riyati by default has adopted an “**opt-out**” approach as explained in section 4.2.2. As per this policy the Patient's Healthcare records are by default viewable by the caregivers. However, Patients have the right to opt-out to stop view of their electronic healthcare records through a consent, collected at the healthcare facility or through the MoHAP Patient portal.

Patient must provide consent each time when he or she visits to a new Healthcare facility. This consent will be collected at the healthcare facility.

4.2.1 Opt-in Consent

In this approach, by default, the patient Electronic healthcare records on HIE require explicit consent from each patient to allow providers to share and access that patient's information via HIE. patient must actively register their consent (Opt-In) to provide access to their Electronic health information to the authorized healthcare professional on Riyati HIE. The consent can be registered at the healthcare facility or through the MoHAP patient portal. Once Patient opts-in healthcare professional can view and access the patient's EHR.

An opt-in Consent may be executed by patient or parent or guardian (in case of minor) or a responsible care giver on behalf of patient.



Once the Opt-in consent is registered at the healthcare facility it will remain active and patient need not to provide consent again for the subsequent visits to the same healthcare facility. In other words, healthcare facility need not to collect the consent for the subsequent visits.

- The data accessed will be subject to:
- usual audit on who accessed the data
- subject to the rules for sensitive data
- subject to the rules for VIP data access
- accessible using “break-the-glass” in case of emergency

4.2.2 Opt-out consent

In the opt-out consent Riayati assume patient consent to allow providers to access patient’s health information but allow patients the opportunity to decline access. Patient has the right to not to allow the care giver to view their EHR through Riayati HIE.

An opt-out Consent may be executed by patient or parent or guardian (in case of minor) or responsible care giver on behalf of patient.

The data accessed will be subject to:

- usual audit on who accessed the data
- subject to the rules for sensitive data
- subject to the rules for VIP data access
- accessible using “break-the-glass” in case of emergency

In this approach the clinicians will be able to access Electronic health records and provide care for patients that present at all the participating healthcare organizations, provided the patient has not explicitly opted out from sharing the data with a particular healthcare facility or across all the healthcare entities connected to Riayati HIE.

This is the preferred approach as it ensures data on Riayati will be available for clinical use and improve the quality of care. This approach is adopted by Riayati HIE.

4.3 Break-the-Glass Access for Emergency Care

Break-the-Glass Access is applicable when Treating a Patient with an Emergency Condition. Patient’s explicit Opt-in consent shall not be required for a Practitioner to access Protected Health Information via Riayati HIE Break-the-Glass to access EHR. If a Break the Glass incident occurred during a patient visit to a healthcare organization, the healthcare organization shall notify the patient of such incident.

Participants healthcare organizations shall inform patients upon discharge from an emergency room if their EHR may have been accessed using Break-the-Glass and inform patients how they may check audit log in the MoHAP’s patient portal to determine if such access occurred.

Break-the-Glass Access provision may be used only if:

- The patient is in Emergency care.
- There is health emergency, and an attempt to obtain consent from patient would result in delay of treatment which would impact the quality of care and increase the risk to the patient’s life or health. During such a situation physician can Break-the-Glass to access EHR.

The participating healthcare organization shall ensure that the access to electronic healthcare records through “break-the-glass” is terminated as soon as the emergency care of the patient is over and a normal consent from the patient can be obtained.



Riyati HIE shall notify patients if their Electronic Health Information was accessed through Riyati HIE without consent. This notice shall include:

- The date and time of the access;
- the healthcare organization from where Electronic Health Information was accessed;
- The name of the Healthcare Professional who accessed the Electronic Health Information;
- The nature of the emergency/ Reason for access

Riyati will monitor and audit Break-the-Glass access logs on a regular basis to prevent any misuse of these provisions.

4.4 Access sensitive Information

Riyati HIE provides special protection for the sensitive health information such as HIV/AIDS, mental health, substance abuse, reproductive health, sexually transmitted disease.

A healthcare provider may access to electronic healthcare information that is classified as sensitive in the Riyati HIE due the medical necessity, wherein the access is required to provide better care to the patient.

Any attempt to break-the-privacy to access sensitive health information will be tracked and audited. The physician shall capture the reason for breaking-the-glass to access Sensitive information.

The clinical applications implemented by participating healthcare organization, used for accessing sensitive information, shall include a warning statement that is viewed by Authorized Users whenever they are obtaining Access to sensitive health information.

Riyati can audit access logs related to access of sensitive health information to prevent any misuse of these provisions.

Health information that are often considered “sensitive” may include:

- **Mental and behavioral health:** Assault, Misconduct, Attempted suicide
- **Reproductive care:** Infertility, Medical termination of Pregnancy, Still birth
- **Substance abuse:** Screening for Amphetamine, Alcohol, Cocaine, Cannabis, MDMA, LSD
- **Diagnosis:** Shyphilis, Chlamydia, Gonohrea, Chandroid, HIV
- **Orders and results:** Barbituarate level screen, Plasma Cholinesterase levels
- **Clinical specialties (for origin of data):** Genetics, Psychiatry, Forensic Medicine
- Medications: Opiates and Narcotics, Injectable Potassium Chloride or Phosphate Concentrate.

MoHAP will maintain and publish updated list of the Sensitive healthcare information and the healthcare data categories, time to time through Riyati portal.



4.5 VIP Patient Data access

The VIP patient data access relates to the confidentiality of EHR of the Patient classified as a VIP patient by the healthcare facility. Special provisions are provided in Riayati HIE related to VIP data confidentiality, access and audit logs.

Healthcare facility must identify a patient as VIP based on the MOHAP's guidelines. The VIP categories can be:

- Royals and Members of Royal Family
- Minister and Senior Members of different Ministries
- Senior ranks in UAE armed forces (e.g. Brigadier)
- Head of UAE Government Departments
- Foreign Delegates and Ambassadors

It is the responsibility of the healthcare facility to identify and mark a patient as VIP based on the criteria published by MoHAP.

MoHAP will maintain and publish complete list of the VIP identification criteria to be followed by healthcare organization

The Healthcare facility shall implement the system such that the VIP healthcare data is shared with Riayati HIE with a VIP flag..

VIP data are considered as highly confidential and will not be accessible to the healthcare provider through Riayati HIE.

4.6 Access for Healthcare Analytics and reporting

Healthcare organizations are required to upload Electronic Health records of all the patients to Riayati HIE as per the guidelines set by the MoHAP. Riayati HIE may make the disclosure to government agencies and MoHAP on behalf of the participating healthcare organization or Patients under applicable UAE laws and regulations

MOHAP may access Electronic Health Information through the Riayati Database, Riayati clinical viewer or provider portal without Consent for public health purposes authorized by UAE laws. Participant's opt-out consent for all or a subset of healthcare facilities in Riayati to access the participant's Electronic Health Information through Riayati shall not prevent or restrict MOHAP from receiving and accessing the participant's Electronic Health Information through Riayati. The purposes of access can be:

- For regulatory reporting and healthcare planning
- To effectively identify and manage disease outbreaks
- For conduction of medical audits
- To investigate suspected or confirmed cases of notifiable diseases and assist in reducing morbidity and mortality
- For the purpose of scientific studies and research for the improvement of the quality of medical care
- For the activities of the Health Emergency identification and Response
- To Disaster Management Organizations, Command Centers during emergency situations
- For the purpose of evaluating and optimizing Healthcare operations and treatment protocols
- For purposes of population health analytics.



4.7 Data De-identification and access for research purposes

De-identification is the process in which patient identifiers are removed to eliminate the possibility of going back to the original data set, this involves removing all identifying data to create unlikable data. The purpose of de-identification and anonymization is to use health care data for research purposes by the Ministry of Health, Universities and other government agencies for improvement on healthcare in the UAE.

Patient consent is not required for Riayati HIE to disclose de-identified Data to MoHAP or by MoHAP approval to any a research organization.

Riayati HIE will provide de-identified data for clinical research purposes after formal approvals and in accordance with the UAE regulations. The proposed purpose of research shall confirm to the definition of clinical research rather than generating market intelligence, competitive advantage, commercial promotion. Sharing Data with any individual who is not a member of the research team is not permitted.

Re-identifying any of the de-identified data by the research team will be done in accordance with the UAE health regulations.



4.8 User Authorization and Access Control

User Authorization and Access control policy governs how a user will be authorized and patient's health information will be accessed by the authorized user.

The participating healthcare organization shall validate the user identity for the purpose of access to Electronic health information through Riayati HIE. The patient healthcare information is a sensitive information. Any unauthorized use (viewing, consuming or transmitting) of EHR must be prevented, and the users of Riayati HIE must be accountable for why and what information is accessed and consumed.

Each healthcare professional shall be uniquely identified by the participating healthcare organization and all their activities tracked while the user is logged on to the system. They must follow a have strict policies and procedures in place to maintain user identities and prevent any misuse of credentials.

The participating healthcare organizations shall identify and categories the users based on their role. Users will get necessary access to the Riayati EHR based on their job function(s), role(s), or location(s), also called Role based Access Control (RBAC).

These healthcare organizations must ensure that the clinical information can only be accessed by the clinical staff responsible for patient care. They do so only in accordance with patient consent and limit their access to information that is relevant to a patient's treatment. They should prohibit unauthorized users from accessing Electronic Health Information in any manner inconsistent with the Policies and Procedure of Riayati.

MoHAP shall publish standard roles for authentication and authorization to be followed by the participating healthcare organizations.

4.9 Audit Logs and Auditing Process

To protect and secure electronic protected health information of a patient Riayati HIE will maintain the Audit logs. These logs will contain all the access events taking place through Riayati HIE such as who is accessing, what data, and for which patient. The log files will be collected, stored, analyzed and reported on a regular basis. This is to ensure the Patient's EHR is only accessed by the authorized Healthcare Professionals for the patient care as per confidentiality and access policy.

Riayati HIE has the authority to monitor and analyze the audit logs on a regular basis. Any suspicious and unwarranted data access shall be reported and acted upon as per the UAE healthcare data privacy regulations. Any authorized access used to access data that is sensitive, VIP, break-the-glass must follow an enhanced auditing process, timely review and reporting.



4.10 Protected Health Information (PHI) Breach Notification

Protected health information (PHI) is any information about health care, or payment for health care that is created or collected by a participating healthcare organization that can be linked to a specific individual. An individually identifiable health information includes patient demographics, Biometrics, radiological images, medical reports, electronic claims and coding, documents and other materials which are stored, shared or accessed through Riayati HIE. This would include any information relating to the past or present physical or mental health of a patient.

Any PHI available on Riayati HIE shall be accessed only by authorized personnel and have required patient consent and only on need basis for providing clinical care or processing of claims. Each Participant shall adopt all the applicable administrative, physical and technical safeguards to prevent any unauthorized access to PHI.

Breach identification:

- Any impermissible access, usage or disclosure of patient healthcare information through Riayati HIE is considered as Breach.
- Access and use of PHI by hospital staff who is not part of the care providing team of the patient is considered a breach.
- Riayati HIE data accessed using the connectivity provided to the participating healthcare organization by a 3rd party contractor or an individual who is not part of the care giver team is considered a breach

In the event of discovery of a breach the participating healthcare organization shall promptly investigate the breach, mitigate the harm, and prevent further breaches. Participating healthcare organizations and providers shall notify MoHAP in accordance with the UAE regulations, at the earliest about a Breach involving PHI access through Riayati HIE. They should assess the scope and magnitude of such suspected Breach and identify the root cause of the breach.

The participating healthcare organization shall develop and implement appropriate safeguards to prevent such breaches. They should also implement necessary controls to respond to PHI breaches.

The participating healthcare organization should investigate and maintain a record of the corrective and preventive actions taken to minimize the risk of future information security breaches.

4.11 Notification Services

While facilitating the sharing of Protected Health Information to provide better quality health care, the privacy and security of patients' data is paramount. Patients can keep track of who accessed the patient Electronics health records.

Notification to Consent: Through consent Patients can control who can access which piece of their electronics health records. Whenever there is any change to patient consent, Riayati HIE will send electronic notifications messages that can be accessed through the patient portal.

Notifications to EHR Access: With this notification service, Riayati HIE provides the patients with notifications whenever EHR is accessed using Riayati HIE by the participating healthcare organizations and Healthcare Professional.