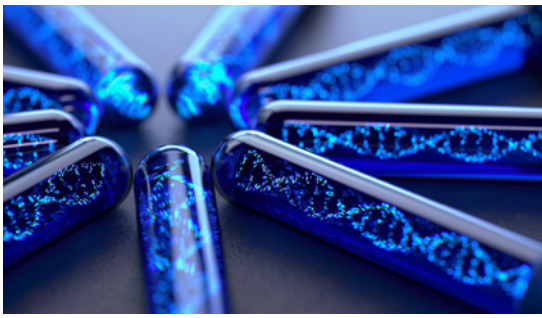
وزارة الصحـــــة العامـــــة
Ministry of Public Health
State of Qatar • دولـــة قطـــر








NATIONAL HEALTH INFORMATION PLATFORM (QHIE-HUB)

ONBOARDING HANDBOOK

National Health Information Platform,
National clinical viewer (eConnect),
e-Prescription and Digital Pharmacy (eMeds),
Registries and Care Plans (eCare)

VERSION 0.3

JULY 2025

Table of Contents

About this handbook 03

Purpose of the onboarding handbook 03

Applying this handbook 04

Navigating this handbook 04

Section A 06
Get familiar with the QHIE-Hub

1 About the QHIE-Hub 07

1.1 Program background & objectives 07

1.2 Overview of National Solutions & their target audience 08

2 Accessing patient data 14

2.1 Patient Consent & Rights 14

2.2 VVIP Data management 16

3 Mandate, key policies & guidelines 18

3.1 MoPH QHIE-Hub Mandate 18

3.2 National eHealth policies 19

3.3 Security policies 21

Section B 24
Get ready to onboard

4 Your readiness journey 25

4.1 The Onboarding roadmap 25

4.2 Pre-Onboarding Assessment 29

5 People and support 31

5.1 Change management toolkit 31

6 Meet the requirements 36

6.1 Security & connectivity 36

6.2 Integration 41

6.3 Data 57

6.4 eMeds: e-Prescription and digital pharmacy 65

6.5 eConnect: National clinical viewer 71

6.6 eCare: registries and care plans 74

7 Ready to onboard 85

7.1 Test workflows in pre-prod 85

7.2 Onboarding Assessment 92

8 Onboarding steps 94

8.1 Connect to the QHIE-Hub Prod environment 94

8.2 Execute historical data migration 94

8.3 Training 108

8.4 Go-Live 115

Section C 120
After You Onboard

9 What to expect after onboarding 122

9.1 Drive adoption and realize benefits 122

9.2 Understand release management 124

9.3 Leverage support & maintenance 125

9.4 Create a business continuity plan 127

9.5 Report security incidents and issues 128

10 Continuous Governance 129

10.1 Monitor data quality 129

10.2 Enable data governance 132

10.3 Data change management for the QHIE-Hub 133

About this Handbook

This chapter outlines the purpose of the onboarding handbook and how to navigate it.

Purpose of the onboarding handbook

Qatar's Health Information Exchange (QHIE) Hub is a national program being implemented by the Ministry of Public Health (MoPH) to facilitate a controlled exchange of healthcare information across stakeholders in the healthcare ecosystem. Its primary objective is to improve clinical outcomes in the State of Qatar.

Implementing such an innovative solution requires all healthcare providers to transform their current operating model to meet the interoperability standards and to securely connect to the ecosystem. The first step in this direction is to understand the requirements of the program and the set of activities that need to be done to get onboarded to the QHIE-Hub. This handbook is intended to be a guide for healthcare providers as they prepare to get onboarded to the QHIE-Hub program across four national solutions, namely the **QHIE-Hub Platform, eConnect: National clinical viewer, and eMeds: e-Prescription and digital pharmacy, and eCare: registries and care plans.** It will familiarize its readers with all the technical requirements of the QHIE-Hub, thereby assisting them throughout their onboarding journey. The handbook will provide guidance interoperability / data standards to be implemented before onboarding, workflow changes to be made, key policies to be followed, and the connectivity as well as data migration activities healthcare providers are expected to undertake as part of their onboarding. It will also provide guidance on the expectations from healthcare providers after they are onboarded and will help them prepare for other national solutions to be released by MoPH in the future.

This onboarding handbook guides healthcare providers through their onboarding journey to the QHIE-Hub program across 3 solutions – the QHIE-Hub Platform, National clinical viewer (eConnect), and e-Prescription and digital pharmacy (eMeds) and Registries and care plans (eCare). It must be used to effectively navigate the overall set of resources / reference documents provided to healthcare providers ahead of their onboarding.

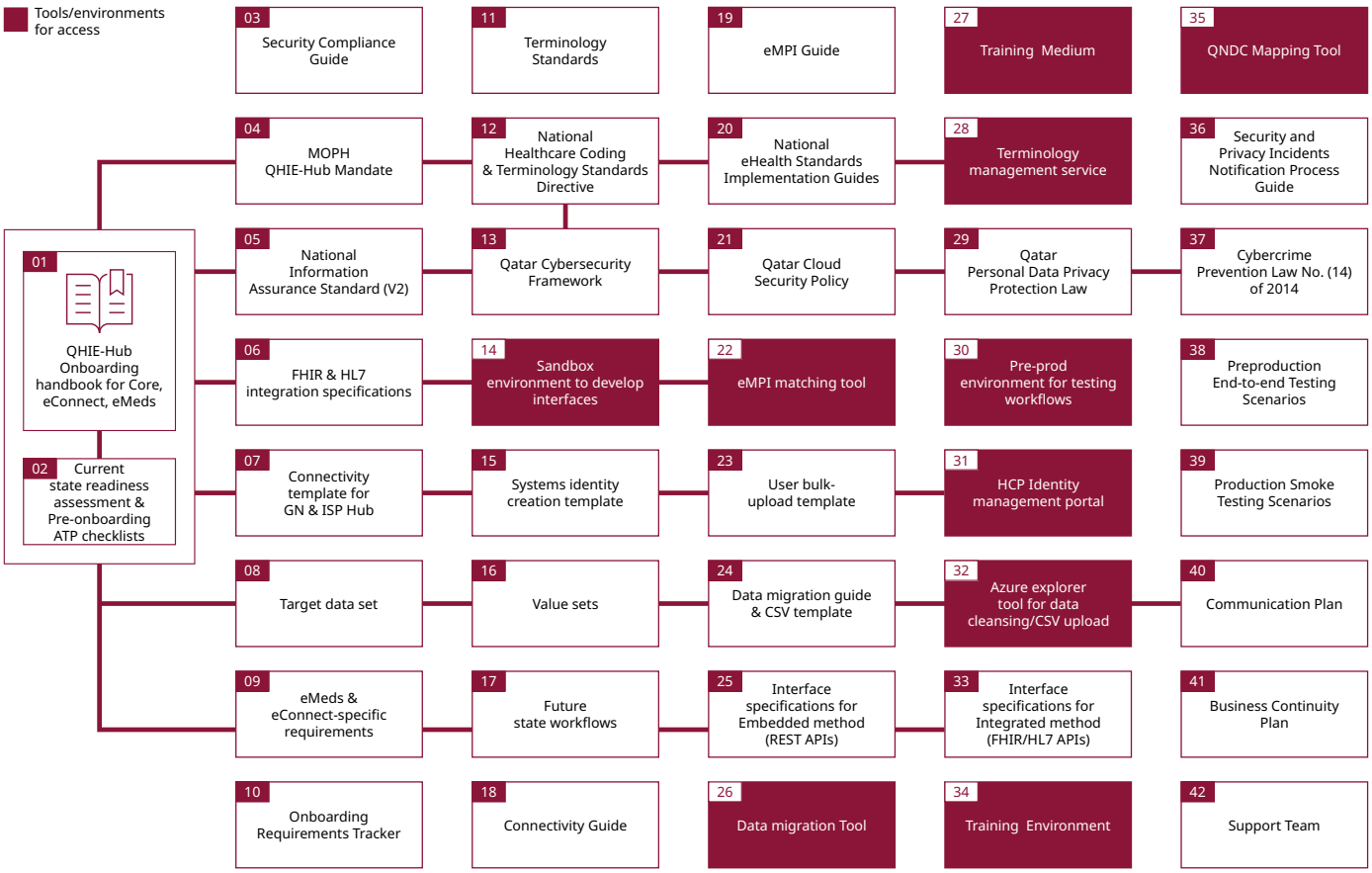


Figure 1. Document hierarchy of the onboarding handbook

Applying this handbook

The onboarding handbook is a part of a larger set of resources provided by the Ministry of Public Health to aid healthcare providers in becoming compliant with the requirements of the **MoPH QHIE-Hub Mandate**. It provides references to other available resources such as the technical standards and guidelines, change management toolkit, training materials, templates, specification documents, portals etc. as outlined in the document hierarchy in Figure 1. As such, healthcare providers must comply with all sections of the handbook and hence, must leverage the document in its entirety. However, based on a healthcare provider's readiness and the phase of implementation, certain sections could be prioritized (e.g., they may refer to specific chapters on connectivity, data, integration, security etc. based on their current state in the onboarding journey).

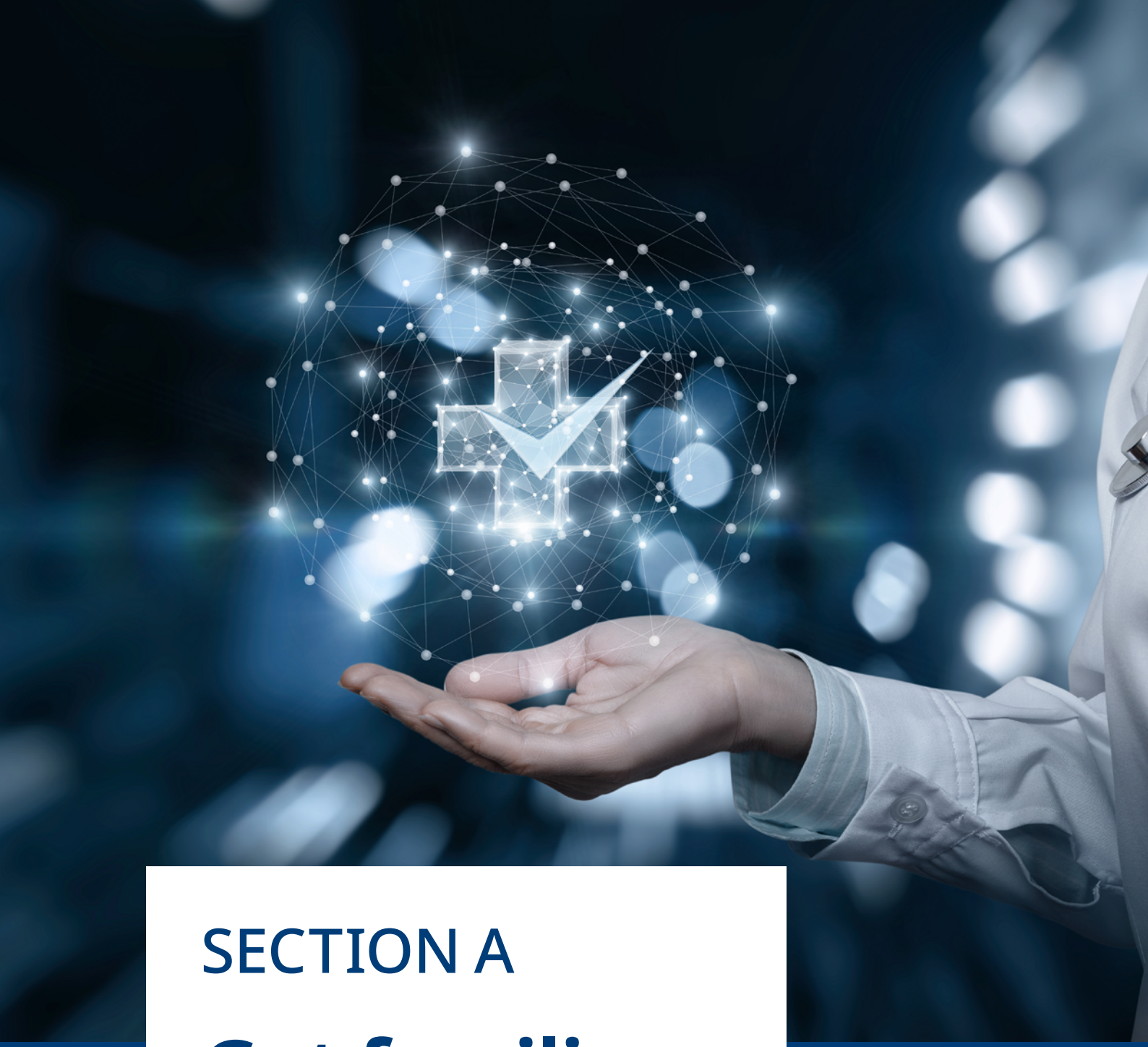
Navigating this Handbook

This handbook has 10 chapters across 3 sections. As a first step, it is recommended that readers go through the full handbook to familiarize themselves with the contents before planning transformation initiatives within their organization.

Once completed, readers may refer to the onboarding roadmap – an image that outlines the sequence of activities that must be completed by a healthcare provider across their onboarding journey. As healthcare providers progress during onboarding, they may refer to the corresponding section in the onboarding handbook for detailed guidance on the expectations in the respective stage and the activities they need to complete.

To help navigate through the document easily and to move across sections or chapters, readers can use the hyperlinks provided at the bottom of every page.


Mandate, policies &guidelines
Overview of national solutions
A. Get familiar with QHIE Hub
B. Get ready to onboard
Onboarding Roadmap
Implementation Plan
Change management
Meet requirements (security, integration, data)
Connect to sandbox to develop APIs
Map & transform data
Clean historical data
Validate patient demographics
Connect to Pre-prod to test workflows
Training
Complete onboarding assessment
Actual onboarding/production
GO LIVE
Go live
C. After you onboard
Drive adoption
Monitor data quality



SECTION A

Get familiar with the QHIE-Hub

CHAPTER 1

About the QHIE-Hub

This chapter provides an overview of the QHIE-Hub, and its national solutions. It also provides additional details on three specific solutions i.e., the National Health Information Platform(QHIE-Hub), National clinical viewer (eConnect), the ePrescription and Pharmacy Network, and the Registries and Care plans (eCare) along with their target audience.

1.1 Program background & Objectives

The Ministry of Public Health (MoPH) has embarked on an ambitious journey to establish a new, integrated model of healthcare delivery in Qatar. This initiative aims to transform the nation's healthcare ecosystem, enhancing both patient experiences and clinician interactions while ensuring higher-value care services. Aligned with the National Health Strategy (NHS) and the broader National Development Strategy (NDS) of Qatar, this transformation reflects MoPH's commitment to advancing healthcare excellence. As a key enabler of this vision, MoPH has implemented a centralized health information repository and exchange platform, formerly known as the Qatar Health Information Exchange Hub (QHIE-Hub), now officially rebranded as National Health Information Platform.

QHIE-Hub, Qatar's first National Health Information Exchange (HIE) Platform, securely connecting healthcare providers across the country. It enables the real-time exchange of critical patient health information through a centralized database of unified patient records and uniform data standards, to support a seamless continuum of care and enhance patient outcomes. It aims to help prevent disease progression, enhance health outcomes, and improve the quality of life for all citizens and residents in Qatar.

As a key pillar of Qatar's national health strategy, QHIE-Hub plays a crucial role in the modernization and digitization of healthcare delivery, integrating both public and private healthcare providers. Every patient interaction—whether a routine consultation, diagnostic test, prescription, or any other clinical encounter—is securely recorded and instantly accessible to patients, authorized providers, and healthcare professionals. By granting healthcare professionals real-time access to comprehensive longitudinal medical records, QHIE-Hub facilitates informed decision-making, strengthens care coordination, reduces unnecessary procedures, and minimizes medical errors, ultimately ensuring a safer, more efficient, and patient-centric healthcare experience. Recognized as one of the most comprehensive and secure National Clinical Viewer (eConnect)platforms

In line with the objectives laid out in the National Health Strategy, MoPH has implemented a central health information platform to facilitate a seamless & secure exchange of healthcare information across the eco-system.

both regionally and globally, QHIE-Hub offers a full suite of national solutions for healthcare professionals, administrators, researchers, and a dedicated patient portal that empowers individuals to manage their health proactively. Developed and managed by the Ministry of Public Health, QHIE-Hub also serves as a central data repository, enhancing the governance and oversight of Qatar's healthcare system by providing greater visibility and regulation of health data. This robust data infrastructure supports evidence-based decision-making and drives the development of policies aimed at improving public health outcomes nationwide

Key objectives of the eHealth strategy:

- **Empower people by transforming their experience:** Ensure accessible, seamless, on-demand services are available across all priority population groups
- **Establish a connected and optimized health system:** Improve digital health infrastructure to establish an integrated and automated health ecosystem
- **Data & analytics-driven health outcomes:** Pivot from reactive healthcare to proactive population health management powered by data and analytics

The aspiration for the QHIE-Hub is to have an integrated journey for the patient, which will empower patients to have enhanced control over their own health information. ***Figure 2 depicts a few examples along this journey.***

Aspiration: An integrated journey

The journey: The national solutions will meet the patient in multiple touchpoints

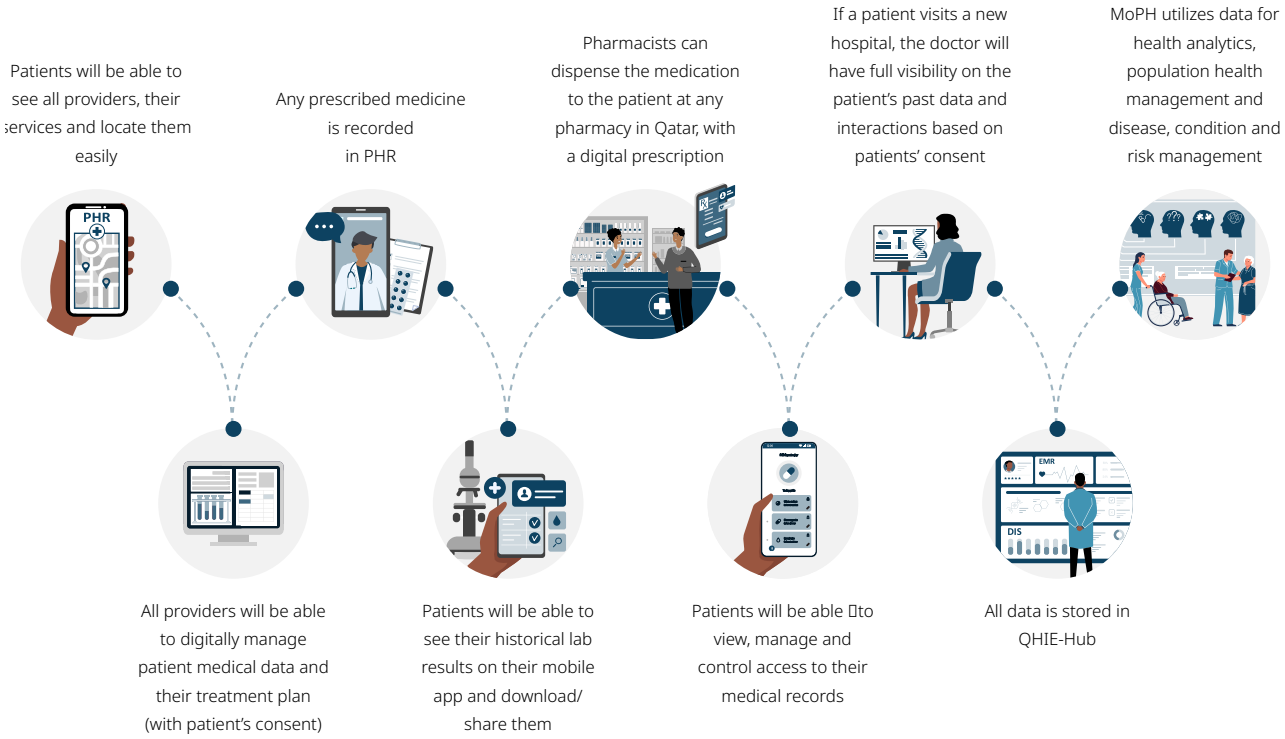


Figure 2. Aspiration: An integrated journey

1.2 Overview of National Solutions & their target audience

The QHIE-Hub hosts eight national solutions for different stakeholders such as patients, providers, pharmacies, etc. It will also provide national decision support capabilities for policymaking via population health management solutions.

Outlined below is a brief overview of these solutions.

Overview of all national solutions:

There are 8 national solutions within the QHIE-Hub targeted at different stakeholders in the healthcare eco-system, collectively aimed at improving patient care and clinical.

1. **National Health Information Platform:** The national central health data repository collects, integrates, and orchestrates all health data exchanges, serving as the backbone for all other digital health solutions.
2. **National Clinical Reviewer (eConnect):** Enables healthcare providers to securely access and review comprehensive clinical data for patients across Qatar, regardless of the healthcare facility
3. **e-Prescription and Digital Pharmacy (eMeds):** A unified system that connects all pharmacies, digitizes prescriptions, streamlines medication dispensing, and minimizes prescription errors

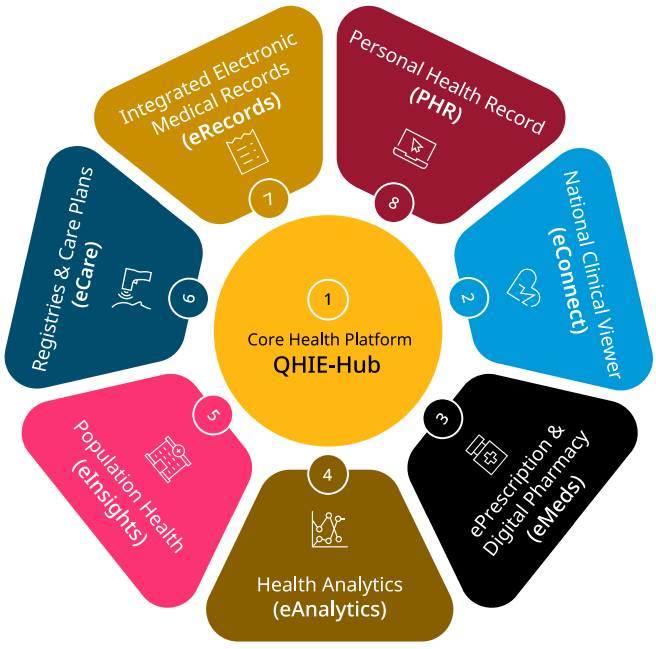


Figure 3. Core Platform/ QHIE Hub

4. **Health Analytics (eAnalytics):** An AI-driven platform designed for research and education institutions, offering secure and anonymized access to health data for advanced analysis and innovation
5. **Population Health (eInsight):** Provides national-level reporting on population health trends, forecasts, and key healthcare statistics to support data-driven policy-making
6. **Registries and Care Plans (eCare):** Establishes standardized care plans aligned with national guidelines and develops national registries for priority populations and health conditions
7. **Integrated EMR Solution (eRecords):** Facilitates the digital transformation of healthcare providers by replacing paper-based records with a secure, electronic medical records (EMR) system
8. **Personal Health Record:** A patient-centric mobile application that grants individuals full control, access, and management of their personal health records

Additional information on the solutions covered in the onboarding handbook:

1. National Health Information Platform (QHIE-Hub)

The QHIE-Hub Platform is a foundational solution that will serve as a gateway to other solutions and provide integration, data storage and transformation capabilities. Consequently, all healthcare providers are required to become compliant with the security and integration requirements of QHIE-Hub Platform and connect to it (directly or indirectly).

Out of these 8 national solutions, requirements for the first four i.e., QHIE-Hub Platform, National Clinical Reviewer (eConnect), e-Prescription and Digital Pharmacy (eMeds), and Registries and Care plans (eCare) will be covered in this document.

It is the backbone of other national solutions that manages a centralized health data repository, creates and maintains unique patient medical records, enables integration, standardization, and secure exchange of health data across healthcare systems / providers.

Key functions of the QHIE-Hub Platform are to:

a. Facilitate the exchange of standardized clinical data from healthcare systems through FHIR and, with temporary HL7 support via APIs available until December 2025

b. Store and manage all patient's health-related data and consent in a central repository for use by other national solutions in a secure manner

The QHIE-Hub Platform is the foundational solution that will serve as a gateway to other solutions. However, healthcare providers will only have access to certain services.

c. Provide MoPH with a centralized management module to manage all national solutions

d. Provide a user management module that creates and manages all user identities across all solutions

e. Store and map all applicable terminology code systems to allow easy data transformation and standardization

f. Create, maintain, and merge patient identifiers to maintain the uniqueness of the patient record

g. Provide audit and monitoring modules that log and track user activities across the QHIE-Hub

h. Expose internal exchange services between QHIE-Hub and other MoPH systems, and across the QHIE-Hub national solutions

i. Provide search and translation services between applicable terminology code systems

Healthcare providers will only be provided access to certain services of QHIE-Hub Platform as outlined below:

- **Enterprise Master Patient Index** – A high-quality, centralized database of all patient demographics in the QHIE-Hub that creates a unique master patient record, can be used to query / create new patients, and is integrated with Ministry of Interior for updates
- **Terminology Management portal** – A portal that enables licensed healthcare providers to download and use mandatory terminology code systems (e.g., SNOMED-CT), standardized value sets, and to host local-to-national cross-maps that enable translation across code systems for interoperability
- **FHIR service** – A gateway to the clinical data repository that consolidates all clinical data and enables a secure exchange through FHIR (Fast Healthcare Interoperability Resources) standards via Application Programing Interfaces (APIs)
- **Rhapsody Integration Engine** – An alternate gateway that accepts patients' electronic health records in HL7v2 (Health Level Seven International Version 2) standards and transforms messages from HL7v2 standard to the target FHIR profile /resources
- **HCP Identity Management portal** – A self-service platform that enables healthcare providers to manage user accounts and roles, generate facility-specific secret keys, and create reports to identify and resolve discrepancies in patient records, ensuring data accuracy and security

All hospitals and clinics that have an Integrated EMR solution (eRecords) system are required to build FHIR / HL7 integration capabilities to integrate with the QHIE-Hub platform. Hospitals or clinics that do not have an EMR have two options:

- Adopt the Basic EMR provided by the QHIE-Hub that is already integrated with the QHIE-Hub Platform
- Adopt a third-party EMR and build FHIR / HL7 integration capabilities to integrate with the QHIE-Hub Platform

Target audience for the QHIE-Hub Platform

Healthcare providers will only be provided controlled access to the above QHIE-Hub Platform services via APIs and no end-user will have access. Additionally, they will also be provided direct access to two portals by designating users to the below roles from their organization:

- **HCP Admin –** Responsible for managing user accounts and roles within the HCP Identity Management Portal, generating secret keys for their facility, and creating

reports to identify and resolve discrepancies in patient records to maintain data accuracy

- **Terminology Author –** A user designated to have access to view published terminology resources and the ability to create or upload new resources (e.g., code systems, value sets and concept maps)

2. National Clinical Viewer (eConnect)

eConnect is a nationwide healthcare solution that provides practitioners with secure access to patient medical records from any healthcare facility in Qatar. By ensuring real-time availability of comprehensive health information, eConnect empowers healthcare providers to make informed decisions, enhance care coordination, and deliver effective, patient-centered care across the country.

eConnect enables practitioners to view a patient's medical records when consent is provided by the patient. It provides a summary of patient's medical history including ongoing diseases, medication, investigations etc.

Key functions of the solution are to:

a. Provides authorized healthcare professionals with read-only access to patient health records upon consent.

b. Displays essential clinical details, including active conditions, allergies, medications, care plans, vaccinations, surgeries, encounter history, and clinical notes.

c. Enables physicians to access a patient's hereditary medical history for informed diagnosis and treatment planning. Lists diagnostic reports, prescribed medications, and clinical documents to support comprehensive patient care.

Target audience for National Clinical Viewer (eConnect):

The following are the different personas within a healthcare provider organization that will have access to National Clinical Viewer (eConnect):

- All physicians, dentists, registered nurses, and clinical pharmacists
- Select Allied Health professionals (limited to Basic Paramedic, Clinical Psychologist, Critical Care Paramedic, Dialysis Technician, Occupational Therapist, Orthopedic Practitioner, Paramedic, Physiotherapist, Podiatrist, Psychological Counselor, Psychologist, Speech Language Pathologist)
- No non-clinical staff (including those in medical administration/IT administration) to be given access

3. e-Prescription and Digital Pharmacy (eMeds)

eMeds is a nationally standardized solution for prescribing, dispensing, and tracking medications, ensuring uniformity across all healthcare providers and pharmacies. It facilitates the electronic issuance, secure dispensing, and real-time monitoring of prescriptions, adhering to national guidelines to enhance medication safety, accuracy, and regulatory compliance.

Key functions of the solution are to:

a. Eliminates the need for paper prescriptions by enabling electronic issuance at a national level

b. Allows patients to have prescriptions dispensed at any pharmacy across Qatar

c. Automatically detects and warns physicians and pharmacists about potential drug-to-drug interactions, allergy risks, and contraindications

d. Displays essential medication details, including images, ingredients, and key prescribing guidelines

e. Alerts practitioners regarding prescriptions for narcotic and psychotropic substances to ensure compliance with regulations

Healthcare providers who have their own prescription module can integrate with eMeds to ensure transactions (e.g., creating prescriptions) occur seamlessly.

f. Allows practitioners to modify prescriptions by stopping, pausing, or adjusting refill dosages as needed

g. Enables practitioners to sign prescriptions electronically, ensuring security and regulatory compliance

The solution comprises three distinct modules:

- **Prescribing Module** – Offers prescribers (e.g., physicians) the necessary functionalities for prescribing medications
- **Pharmacy Module** – Enables pharmacies by providing them with essential dispensing information and functionalities
- **Management Module** – Accessible to authorized users from MoPH to administer or configure prescribing / dispensing rules; also accessible to hospitals/pharmacists in limited capacity to navigate and view drugs as well as active substances

Target audience for eMeds:

The following are the different personas within a healthcare provider organization that have access to ePrescription and Pharmacy Network (eMeds):

- All Physicians, Dentists will have full access to the Prescription module
- Residents, Physiotherapists, Dental Trainees, Nurse practitioner will have access to the Prescription module, but will require a co-sign to prescribe
- No nurse, Allied Health Professionals, or non-clinical staff (including those in medical administration/IT administration) to be given access to any module
- All pharmacists will have access to the Pharmacy module

4. Registries & Care Plans (eCare)

eCare is a national healthcare solution designed to establish disease and condition registries and develop patient-specific care plans aligned with national clinical guidelines. It enhances disease management by ensuring that patients receive personalized, evidence-based care tailored to their specific health needs, improving treatment outcomes and continuity of care.

Key functions of the solution are to:

a. Display registries of patients with relevant demographic and clinical information (e.g., age, diagnosis, disease state) at a level appropriate to user's role

b. Assess behavioral and clinical risk factors of patients to give recommendations based on national clinical guidelines (e.g., treatment protocols, follow-up schedules, referral to specialists, patient education materials)

c. Highlight potential drug interactions between current medications of patients and new medications recommended by healthcare providers

d. Allow healthcare practitioners to set personalized treatment and lifestyle management goals for their patients

e. Enable healthcare practitioners to select educational materials and questionnaires from a library of approved resources and subsequently to print or share them with their patients via the national Personal Health Record App (PHR) solution

f. Allow healthcare professionals to message members of care teams and their patients for better care coordination

g. Display reports on disease trends and progression at a level appropriate to user's role

The solution comprises of two distinct modules:

- **Care Plan and Registry Module** – Offers selected healthcare professionals the ability to create and manage care plans of their patients with targeted chronic diseases and/or conditions after adding them to relevant national disease registries, and view national disease registries and their summaries at a level appropriate to their role
- **Reports and Statistics Module** – Offers selected healthcare professionals the ability to view statistics and clinical reports related to care plans and disease registries for targeted healthcare conditions

Target audience for Registries & Care Plans (eCare):

The following are the different personas within a healthcare provider organization that will have access to the Registries and Care plans (eCare) solution:

- Physicians will have full access to only those care plans, disease statistics, and registries relevant to their scope of practice
- For other diseases, physicians will have read-only access to care plans regardless of their practice (except laboratory medicine, ultrasound, and forensic medicine physicians who will not have any access)
- Clinical nurses will have full access to only those care plans and registries relevant to their scope of practice
- Other nurse practitioners and select allied healthcare professionals will have read-only access to care plans relevant to their practice
- No dentists and pharmacists will be given access to the solution
- Heads of clinical departments, as a supervisor, will have read-only access to care plans, disease statistics, and registries at the department level
- Heads of healthcare facilities, as a supervisor/ manager, will have read-only access to care plans, disease statistics, and registries at the facility level

Only registered practitioners who have an active DHP license will be provided access to National clinical viewer (eConnect). Healthcare professionals, including trainees, are allowed to access ePrescription and Pharmacy Network (eMeds) and Registries and Care plans (e Care) solutions based on their role.

At the time of onboarding to any of the above-mentioned solutions, healthcare professionals and their roles will be verified with details from the Department of Healthcare Professionals (DHP) before providing access to the solutions.

*****

CHAPTER 2

Accessing patient data

This chapter informs the reader about how patient data is classified and accessed across the QHIE-Hub solutions. It covers the following topics:

1. **Patient consent and rights**
2. **VVIP data management**

2.1 Patient Consent & Rights

Patient privacy and confidentiality are of utmost priority within the QHIE-Hub. All individuals must have full control over how their healthcare information is shared. This is the most important design principle of the consent management workflows within the QHIE-Hub.

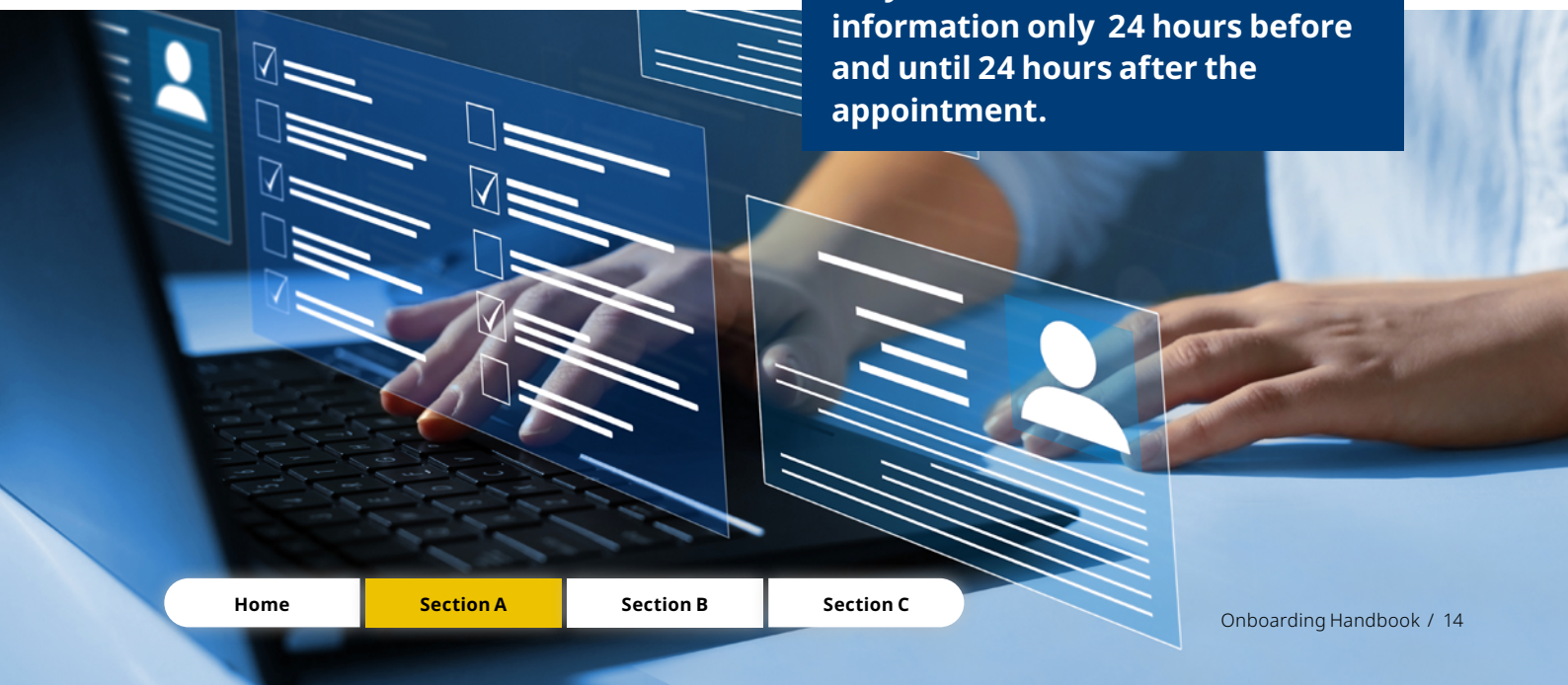
There are three levels of patient data stored in the QHIE-Hub:

- **Protected health information** – Any health data that includes identifying information (e.g., name, address, clinical data including health conditions, diagnosis, medication etc.)
- **Clinical data** – Information about the medical condition or treatment of patients which has the potential to cause direct and indirect harm (e.g., biological, psychological and / or social harm if leaked).
- **Sensitive clinical Data** – A sub-category of diseases or conditions, and their affiliated health data (e.g., diagnosis, diagnostic investigations, medication etc.); this includes sexually transmitted infections, premarital screening, mental health disorders (bar suicidality and self-injury).

How consent will be applied within the QHIE-Hub:

- All individuals' data by default is shared with MoPH into the QHIE-Hub. Consent Settings are then applied to determine how their data is shared with healthcare providers across Health Information Exchange, ePrescription and Digital Pharmacy (eMeds), and Registries and Care plans (eCare) solutions.
- There will be default settings for sharing data with healthcare providers for all patients. However, all patients have the option to change these share settings at any time through their Personal Health Record App profile.

Based on consent settings, practitioners can access non-sensitive clinical data of a patient from 48 hours before the appointment till 45 days after the appointment. However, they can access sensitive clinical information only 24 hours before and until 24 hours after the appointment.



- **Default setting for access to clinical data** for all patients except VVIPs (excluding sensitive data):
  - Data will be shared with **treating healthcare organizations** (i.e., with all eligible healthcare practitioners in the facility with which a patient has an appointment) if the appointment is with a public or semi-public sector facility, a private general hospital or a diagnostic and treatment center.
  - However, data will only be shared with the **treating healthcare practitioner** if the appointment is with any other type of facility.
  - The consent duration will **start 48 hours before the appointment is scheduled and will end after 30 days from the date of the appointment**, after which time the data will no longer be viewable (until another appointment date, which then opens another 30 days viewing ability of the health data). If providers need to access this data beyond the above duration, they will need a patient's consent again.
  - Patient can choose to change the default setting, in which case the data will not be shared with the treating healthcare organization (or any organization)
- **Default setting for access to sensitive clinical data** for all patients except VVIPs:
  - Data will be shared with **the treating healthcare practitioner only** (the one specific practitioner that the patient has an appointment with)
  - The consent duration for sensitive clinical data will **start 24 hours before the appointment is scheduled and will end 24 hours after the appointment**, after which time the data will no longer be viewable
  - Patient can choose to change the default setting, in which case the data will not be shared with the treating healthcare practitioner (or any practitioner / provider)
- **One Time Access Consent and Break-the-Glass Access**
- Irrespective of the patient's consent settings, there will always be 2 options to access the data if required
  - One Time Access Consent, which is requested from the Practitioner and requires an OTP from the patient to allow access to their data (either sensitive or non-sensitive clinical data)
  - Emergency Access or Break-the-Glass Access which can be activated in emergency situations where the patient is unable to give consent and it is critical for patient care. Under these circumstances, following the resolution of the emergency, patients will have full transparency on who accessed which of their data.

Key scenarios governing a practitioner's access to a patient's sensitive and non-sensitive data:

1. **Direct access (when a patient has given consent to share both sensitive and non-sensitive information)**

This will be the default setting for the Personal Health Record App and will apply even to those individuals who have not logged in

a. A practitioner can preview non-sensitive information from the patient profile on Health Information Exchange.

b. The practitioner may also access sensitive information 24 hours before and after the appointment.

c. If consent to share non-sensitive or sensitive data is not provided, practitioners may request patients for permission to access this data. Doing so will send a one-time password to the patient's mobile number which needs to be shared with the practitioner (who needs to enter it within Health Information Exchange for validation).

2. **Request access permission (when a patient has not given any consent)**

a. A practitioner needs to login and request permission to access non-sensitive data. Doing so will send an access code to the patient's stored mobile number which needs to be shared with the practitioner

(who needs to enter it within Health Information Exchange for validation).

b. A practitioner needs to follow the same process again in case access to sensitive data is also required.

3. **Emergency break-the-glass access**

a. A practitioner needs to select Emergency break-the-glass (EBG) access option in Health Information Exchange. This request needs to be validated by the healthcare provider. Once validated, the practitioner can access all patient clinical information including sensitive data only for one session. Once the access window is closed, access will be revoked.

b. The above process needs to be re-initiated if access is needed again (via a new session).

2.2 VVIP data management

One of the critical business workflows healthcare providers need to modify as part of their onboarding is how VIP and VVIP data is managed and shared with the QHIE- Hub.

The QHIE-Hub will maintain a centralized list of VVIPs. Only individuals within this list will be classified as VVIPs (irrespective of their status within the HCP).

The Ministry of Public Health has determined that VVIPs also require quality clinical care, and therefore, their data needs to be collected and stored in the QHIE-Hub. As part of the Enterprise Master Patient Index (eMPI) service, the QHIE-Hub will obtain a list of VVIPs from official sources. **Only individuals within this list will have the VVIP status**. All other individuals, irrespective of whether they are deemed VIP or VVIP by a healthcare provider, will be treated as any other patient within the QHIE-Hub.

The QHIE-Hub requires true identifier information (i.e., QID / GCC ID / Passport number), nationality and date of birth (at minimum) to query patients.

- QID + Birth date
  (for residents and citizens)
- GCC ID + Nationality + Birth date
  (for GCC residents and citizens)
- Passport number + Nationality + Birth date
  (for other nationality citizens)

There are three scenarios possible during patient search / registration of a patient:

1. **When a patient is categorized as a VIP or VVIP by the healthcare provider <u>AND IS</u> a VVIP in the QHIE-Hub:** The healthcare provider registers the patient as per their current VIP / VVIP registration process. When the patient is searched using the eMPI service of the QHIE-Hub, an acknowledgement with limited information is returned to the healthcare provider.
2. **When a patient is categorized as a VIP or VVIP by the healthcare provider <u>BUT IS NOT</u> a VVIP in the QHIE-Hub:** The healthcare provider registers the patient as per their current VIP / VVIP registration process. When the patient is searched using the eMPI service of the QHIE-Hub, all demographic information is returned like any other patient to the healthcare provider.
3. **When a patient is <u>NOT</u> categorized as a VIP or VVIP by the healthcare provider <u>AND IS</u> a VVIP in the QHIE-Hub (an unlikely scenario):** The healthcare provider registers the patient as per their regular registration process. When the patient is searched using the eMPI service of the QHIE-Hub, an acknowledgement with limited information is returned to the healthcare provider.

Key considerations for healthcare providers to develop VVIP patient workflows:

- The QHIE-Hub will consider the QID / GCC ID / Passport number, nationality and the date of birth as unique identifiers to register a patient by mapping data from all hospitals against these attributes. All individuals, irrespective of whether they are deemed VIP or VVIP by a healthcare provider, will be treated as any other patient within the QHIE-Hub. Hence, they will have same querying, updating and registration workflows like any other patients and healthcare providers must ensure demographic information is accurate for all registered patients.

- During registration, a healthcare provider may query a VVIP patient using their identifier information (i.e., QID / GCC ID / Passport number), nationality and date of birth as per the current process. However, unlike other patients, the QHIE-Hub will only return the **identifier number, date of birth, gender, and nationality for a VVIP patient in QHIE-Hub.** All other demographic information (e.g., name/address/phone number etc.) will be excluded.
- Default setting for VVIP data access is that it is **NOT shared**, without explicit access consent approval from the VVIP (across all data categories). Hence, a treating physician querying this information on Health Information Exchange may not be able to get any heath information in case a VVIP has not provided consent. However, the physician may choose to request this information via OTPs as per the consent management workflows.
- VVIP patients may change their consent settings by enrolling within Personal Health Record Application via the standard process or by utilizing the manual registration process for identity proofing. They may control the sharing of all information via the Personal Health Record Application consent module.
- Once access is approved by VVIP, access will be given to clinical practitioners when required to provide quality clinical care via the Health Information Exchange solution for the pre-defined duration.
- A practitioner accessing the VVIP record within Health Information Exchange will only be able to see the **identifier number, date of birth, gender, nationality, NHN number & blood group** for the VVIP patient (**if consent is available**).
- All VVIP information will be classified at C4 level of confidentiality within the QHIE-Hub. Healthcare providers are required to implement the same at their end along with the necessary security controls prescribed by National Information Assurance (NIA).

*****

CHAPTER 3

Mandate, key policies & guidelines

This chapter outlines the key policies and mandates that all healthcare providers must adhere to before onboarding to the QHIE-Hub. It provides a comprehensive overview of regulatory requirements, technical standards, and implementation guidelines across data, integration, and security domains, as mandated by the Ministry of Public Health (MoPH).

3.1 MoPH QHIE-Hub Mandate

In alignment with Qatar National Vision 2030 and the objectives of the National Health Strategy, the Ministry of Public Health (MoPH) has mandated the immediate integration of all healthcare facilities with the National Health Information Exchange Platform (QHIE-Hub). Compliance with this directive is a prerequisite for obtaining and renewing healthcare facility licenses from MoPH.

The mandate covers several key topics related to data sharing within the State of Qatar, adoption of the QHIE-Hub, data quality, patient privacy and confidentiality, and security.

Implication of the mandate are:

- Healthcare providers must share the QHIE-Hub related patient health data and continuously update the QHIE-Hub in real-time or as per the frequency specified by MoPH. For this, they must accurately record, transform, and clean the required data (including historical data for the prescribed duration) in their health information system(s) as per the defined data sets and National Coding and Terminology Standards Directive
- Healthcare providers must exchange and transmit (including build capabilities to send and receive) data to the QHIE-Hub using the data exchange standards and APIs defined by MoPH. They must also prepare their health information systems to integrate with the QHIE-Hub platform as per QHIE-Hub specifications
- Healthcare providers must integrate with the National Master Patient Index (aka eMPI) service within their system(s) and configure their systems to store National Health Number
- Healthcare providers must follow the onboarding process as defined by MoPH and provide all necessary information for the QHIE-Hub system configuration, such as system user information, HCP administrator, workflow configuration information, and baseline data
- Healthcare providers must provide necessary human resources for integrating their local systems with the QHIE-Hub and the associated national solutions. For example, they should designate lead trainers and should participate in Train-the-Trainer sessions conducted by MoPH

All HCPs are required to be compliant with the MoPH QHIE-Hub mandate and related policies across data, integration and security before onboarding to the QHIE-Hub.

- Healthcare Providers must choose one of the available ways to utilize the e-Prescription and Digital pharmacy Network Solution for all their prescription and dispensing activities for supported workflows
- Pharmacies using electronic systems to fill, create, store, and / or track prescriptions must share these transactions with the QHIE-Hub and facilitate two-way communication (sending and receiving messages) with the QHIE-Hub for prescription information, pharmacy decision support, and notifications.
- Healthcare Providers must enroll applicable patients who have any of the diseases and/or conditions covered by a national registry into the Registries and Care Plans (eCare) solution using the available integration ways

The detailed mandate is available as a reference along with the onboarding handbook.

3.2 National eHealth policies

With reference to the above mandate and MoPH's plan to implement other national solutions such as Qatar Health Insurance Solution (QHIS), and Qatar Pharmaceutical Track and Trace System (QPTTS), healthcare providers are required to adopt the national policies and standards outlined below.

Table 1. Mandated national standards

Domains		Mandated National Standard	Version
Diagnosis	Administrative / Billing	ICD-10-CM	2025 edition
	Clinical	SNOMED CT	20241101 Int. Version
Laboratory	Clinical (Orders / Results)	LOINC	2.78
	Billing	CPT	2024
Immunization	Clinical	CVX	2024 version
	Billing Vaccine	QNDC	Latest version
Allergy	Drug Allergies	QNDC + SNOMED CT specific code set	Latest version
	Food Substance / Environmental Allergies		W20241101 Int. Version
Procedure	Outpatient Services and Procedures	CPT	2024
	Inpatient Services and Procedures	CPT	2024
	Other Medical Services (e.g., Medical Equipment and Supplies)	HCPCS	2024
Radiology/Imaging	Clinical (Orders / Results)	LOINC	2.78
	Billing	CPT	2024
Pharmacy	Drug Code / Classification (Clinical and Billing)	QNDC	November 2024
	Logistics (Pharma Products)	GS1 – GTIN	Latest version - QNDC
Dental	Procedures (Clinical and Billing)	ASDSG 12th Edition	2024
	Clinical Diagnosis	SNOMED CT (SNODENT Ref Set)	20241101 Int. Version
Clinical Observation (e.g., Vitals)	Clinical	LOINC	2.78

HCPs are required to be compliant with national e-health policies such as the Qatar National Healthcare Coding and Terminology Standards Directive, along with other data policies.

1. Qatar National Healthcare Coding and Terminology Standards Directive

This policy lays the foundation for achieving semantic interoperability to share health information among Provider Systems and integrating health data with national solutions to provide better care to the public of Qatar.

It specifies the following coding and terminology standards approved by National eHealth Data Quality, Standards, and Policies sub-Committee for use in the State of Qatar. All the billing / insurance coding standards have been approved by the Qatar National Clinical Coding Committee (QNCC).

The mandated coding standards must be fully implemented by May 31, 2025. The updated mandated coding standards and versions are as follows:

License requirements as part of the directive:

- Certain coding standards from the above-mentioned table such as ICD-10-CM, LOINC, CVX are free to use.
- MoPH has procured SNOMED CT, CPT, and HCPCS at the national level, making them available upon request through the designated access procedures outlined in the National Mandated Standards Reference Guide.
- MoPH will provide the licenses for certain Code Systems: IR-DRG and ASDSG 12th Edition.
- MoPH has already published Qatar specific national standards: QNDC, QACS (formerly known as QOCS).

All healthcare providers must start preparing to adopt the National Coding and Terminology Standards as defined in the Qatar National Healthcare Coding and Terminology Standards Directive, which was published on January 1, 2023, and is available on the MoPH website. The implementation deadline for mandatory medical coding was published on February 24, 2025, with a compliance deadline of May 31, 2025.

For further details, providers should refer to the MoPH website or contact **medicalcoding@moph.gov.qa.**

2. Qatar National eHealth Standards Implementation Guides

To drive adoption of the Qatar National eHealth Standards (QNeHS), MoPH is publishing implementation guides that define how these standards can be implemented within Health Information Systems. These guides describe how the national standards are defined, used, licensed, and implemented. They also provide the implementation approach, key activities and resources required for the implementation, official websites, and other resources.

Implementation guides for the standards are available for the following domains:

- Diagnosis
- Laboratory
- Immunization
- Allergies
- Procedures
- Radiology
- Pharmacy
- Dental
- Clinical Observation

3. Other data policies

To ensure controlled usage of the QHIE-Hub data for intended outcomes while safeguarding the privacy of individuals, MoPH will continue to publish other relevant policies over time. These may include:

- **Data confidentiality policy:** The purpose of this policy is to establish the conditions under which privacy and confidentiality measures for individuals as patients or clients is established, used, asserted and / or revoked across the health sector in Qatar.
- **Person Identity Management Policy:** The purpose of this policy is to establish the conditions under which identity for

healthcare documentation for persons as patients or clients is established, used, asserted and / or revoked across the health sector in Qatar.

- **User Identity Management Policy:** The purpose of this policy is to establish the conditions under which identity for individuals as users of IT systems is established, used, asserted and / or revoked across the health sector in Qatar, subject to policy scope
- **Practitioner Identity Management Policy:** The purpose of this policy is to establish the identity of individuals as Practitioners who are registered with a valid and current license from DHP.
- **Data Security and Audit Policy:** The purpose of this policy is to establish the conditions under which Personal Health Information (PHI) is protected, secured, and audited by authorized individuals across the health sector in Qatar.
- **Data Use Policy:** The purpose of this policy is to establish the conditions under which Protected Health Information (PHI) is defined, captured, viewed, used, protected and / or exchanged across the health sector in Qatar

3.3 Security policies

Onboarding to the QHIE-Hub requires healthcare providers to comply with all Qatar-wide health privacy and cybersecurity laws and regulations, specifically those focused on protecting and/or securing PHI and PII. All healthcare providers are expected to understand the existing laws/ regulations/standards and implications for their organization to develop and implement necessary internal security policies to protect data throughout all stages of the data lifecycle.

Following is a list of the National cybersecurity policies / regulations that healthcare providers need to consider as they develop a comprehensive list of security controls and policies:

- **National Information Assurance Standard (V2)** – The National Cyber Security Agency (NCSA) has designed and created the policy titled "National Information Assurance Standard" as a guide for all government and private sector organizations within Qatar. It outlines baseline controls that organizations should implement at a minimum to:
  - Protect information assets and systems
  - Effectively manage information cybersecurity risks
  - Achieve regulatory compliance for international standards certifications (e.g., ISO 27001)
- The NIA Standard is designed to be used in conjunction with the National Data Classification Policy [IAP-NAT-DCLS] and applicable laws and regulations within the State of Qatar. Together the two documents will help organizations in implementing a robust information security management system within their organization.

  The policy documents can be found here:
  - National Information Assurance Standard [IAS-NAT-INFA]
  - National Data Classification Policy [IAP-NAT-DCLS]
- **Qatar Cybersecurity Framework –** The Qatar 2022 Cybersecurity Framework was developed by the Supreme Committee for Delivery & Legacy. It aims to adopt an innovative, capability-based, fit-for-purpose approach. It considers security risks identified by the entities during risk management and uses it to scope services and associated systems. The framework is designed to focus on raising and embedding "must-have" capabilities and competencies required by all entities that are part of the ecosystem. It takes into consideration the current maturity levels of entities in Qatar, the current / future challenges and builds on the existing cybersecurity laws, standards, and competencies within Qatar.

  The policy document can be found here: Qatar 2022 Cybersecurity Framework

HCPs need to be compliant with all the data protection and cyber security laws such as NIA before they are onboarded to QHIE-Hub.

- **Qatar Cloud Security Policy–** The cloud security policy is developed by MOTC to provide an overview of cloud computing as well as the security and privacy challenges involved. The policy discusses the threats, technology risks, and safeguards for cloud environments. The objective of this policy is to make sure that the usage of cloud services is in accordance with the business and security requirements as well as relevant laws and regulations.

  The policy document can be found here: Cloud Security Policy

- **Qatar Personal Data Privacy Protection Law** – The Qatari Law No. 13 of 2016 ("the Personal Data Privacy Protection Law") took effect in 2017, with the aim of protecting and providing guidelines for processing personal data within Qatar. In December 2020, the Compliance and Data Protection Department (CDP) within the Ministry of Transport and Communications (MOTC) published new guidelines in relation to the Law. The scope of the PDPPL applies to personal data that is received, collected, extracted, or processed through electronic or traditional methods. Any organization that processes such personal data must adhere to the principles of transparency, fairness, and respect for human dignity.

  The policy document can be found here: Personal Data Privacy Protection Law

- **Cybercrime Prevention Law No. (14) of 2014** - On 16 September 2014, the Qatari government promulgated a cybercrime prevention law (No.14 of 2014) to increase the tools for combating online and cybercrimes. The new law imposes many sanctions and several penalties for offences committed through the Internet, IT networks, computers, and other related crimes. The legislation is aimed at safeguarding the country's technological infrastructure and strengthening cyber security within Qatar.

- **Other cloud security policies** such as MCIT Cloud Security Policy v1.3, Azure Qatar Reference Architecture and Microsoft Cloud Adoption Framework, to ensure that provisioning of cloud services within their organization is in accordance with the security requirements as well as relevant laws and regulations.


You are here
Mandate, policies &guidelines
Overview of national solutions
A. Get familiar with QHIE Hub
B. Get ready to onboard
Onboarding Roadmap
Implementation Plan
Change management
Meet requirements (security, integration, data)
Connect to sandbox to develop APIs
Map & transform data
Clean historical data
Validate patient demographics
Connect to Pre-prod to test workflows
Training
Complete onboarding assessment
Actual onboarding/production
Go live
GO LIVE
C. After you onboard
Drive adoption
Monitor data quality

SECTION B

Get Ready to Onboard

CHAPTER 4

Your Readiness Journey

4.1 The onboarding roadmap

Onboarding of a healthcare provider to the QHIE-Hub involves 5 key stages across 3 key phases in the journey as outlined in the onboarding roadmap:

1. **Pre-onboarding phase**
    a. Get familiar with the QHIE-Hub
    b. Identify and report gaps
    c. Transform yourself
2. **During onboarding phase**
    a. Actual onboarding & integration
3. **After onboarding phase**
    a. Maintenance & continuous improvement

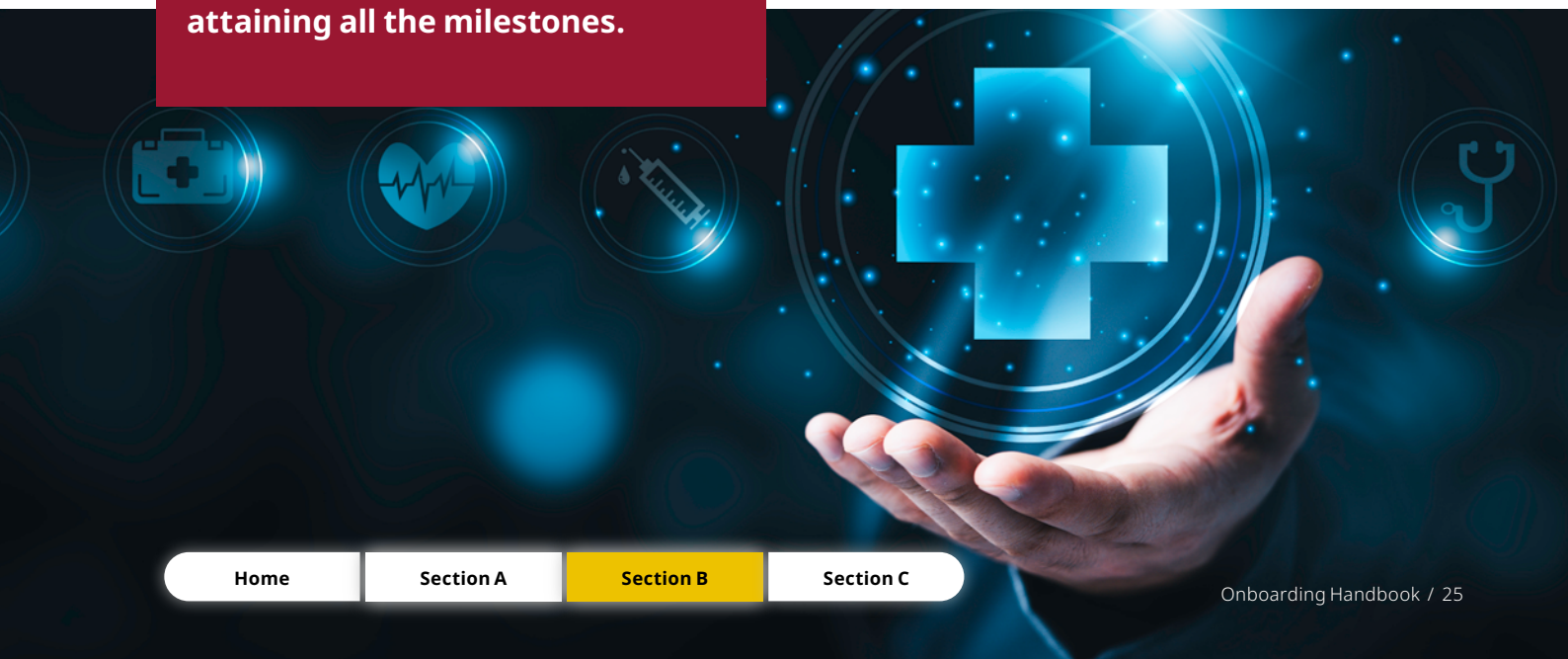
Across this journey, there are multiple checkpoints with clearly defined outcomes that healthcare providers must achieve to move forward. This chapter provides details about the milestones in the onboarding journey along with their exit criteria to ensure healthcare providers can carefully plan and execute various activities in every stage. It also outlines the onboarding reviews that will be conducted by MoPH to assess a healthcare provider's progress in this journey.

Onboarding process of a healthcare provider to the QHIE-Hub requires completion of multiple activities across different phases. These phases have clearly defined exit criteria and milestones. No healthcare provider will be onboarded without attaining all the milestones.

Pre-onboarding

This phase includes the first three stages i.e., get familiar with the QHIE-Hub, identify and report gaps, and transform yourself. There are 8 key milestones (Milestone 1 – Milestone 8) healthcare providers need to achieve which are detailed in this section.

- **Milestone 1 (Kick-off):** The kick-off milestone marks the beginning of the onboarding journey for healthcare providers (HCPs). At this stage, HCPs should familiarize themselves with the QHIE-Hub, assess their implementation readiness, and establish a structured approach for onboarding. This includes reviewing key reference materials, identifying gaps, and setting up a dedicated change management team to drive the process forward.



To cross this milestone, a healthcare provider should complete the following tasks:

- Review the onboarding handbook, journey documents, and implementation plan template
- Access the exchange medium by using the provided link and guide
- Conduct a gap analysis and define target completion timelines
- Establish a change management team with clear roles and responsibilities
- Start implementing measures to comply with all security & infrastructure requirements of the QHIE-Hub

- **Milestone 2 (Develop APIs and connect to the sandbox to validate):** In this step, a healthcare provider should connect their non-production system to the QHIE-Hub's sandbox environment. This environment will be used by healthcare providers to validate APIs they have developed for the QHIE-Hub interfaces and to validate data migration pipelines. They can leverage the API Developer portal along with other resources (e.g., interface specifications) to meet requirements of this stage. However, healthcare providers should only use synthetic data in this environment and must ensure actual PHI / PII is not shared with the QHIE-Hub. To cross this milestone, a healthcare provider should complete the following tasks:
  - Connect to the QHIE-Hub's sandbox environment via the Government Network or ISP Hub; compliance with the security & infrastructure requirements is a pre-requisite
  - Prepare and connect the API client service to validate the QHIE-Hub interfaces
  - Develop integration workflows (e.g., to query, retrieve, or create patient records)
  - Develop data migration pipelines to send historical and real data
- **Milestone 3 (Map and transform data):** This step can be done in parallel to the activities in the previous milestone. In this milestone, a healthcare provider must start collecting and transforming their historical data as well as their source systems generating real-time data to meet the QHIE-Hub's target data sets and business rules. To cross this stage, a healthcare provider should complete the following tasks:
  - Complete terminology mapping for historical and real-time data
  - Organize historical data as per target datasets and business rules
  - Execute data profiling and cleaning techniques
- **Milestone 4 (Validate patient demographics):** In this milestone, a healthcare provider should start utilizing the benefits of eMPI tool of the QHIE-Hub to validate their full patient database against the Ministry of Interior's database. However, activities in Milestone 3 i.e., organizing data as per target datasets, applying business rules need to be completed before this step (at a minimum for patient demographics e.g., gender, nationality etc.). In this stage, healthcare providers should use real demographic data of their patient records.To complete this step, the healthcare provider must achieve full compliance by meeting the minimum required percentage for accurate matching of patient demographic details.
- **Milestone 5 (Clean historical data):** There are two available approaches for historical data migration: CSV-based migration and API-based migration. If the API approach is chosen, a healthcare provider should follow the Testing Clinical Data Guide to load resources using the developed APIs. Before proceeding, the development phase must be fully completed, ensuring that all APIs are configured correctly and aligned with the QHIE-Hub's data requirements. During this step, the provider must verify that API responses return no errors, confirming that the data is accurately structured and meets the defined compliance standards. If a healthcare provider chooses the CSV approach, can use the data migration tool to clean their historical data. The data migration tool will connect to an Azure Storage account where

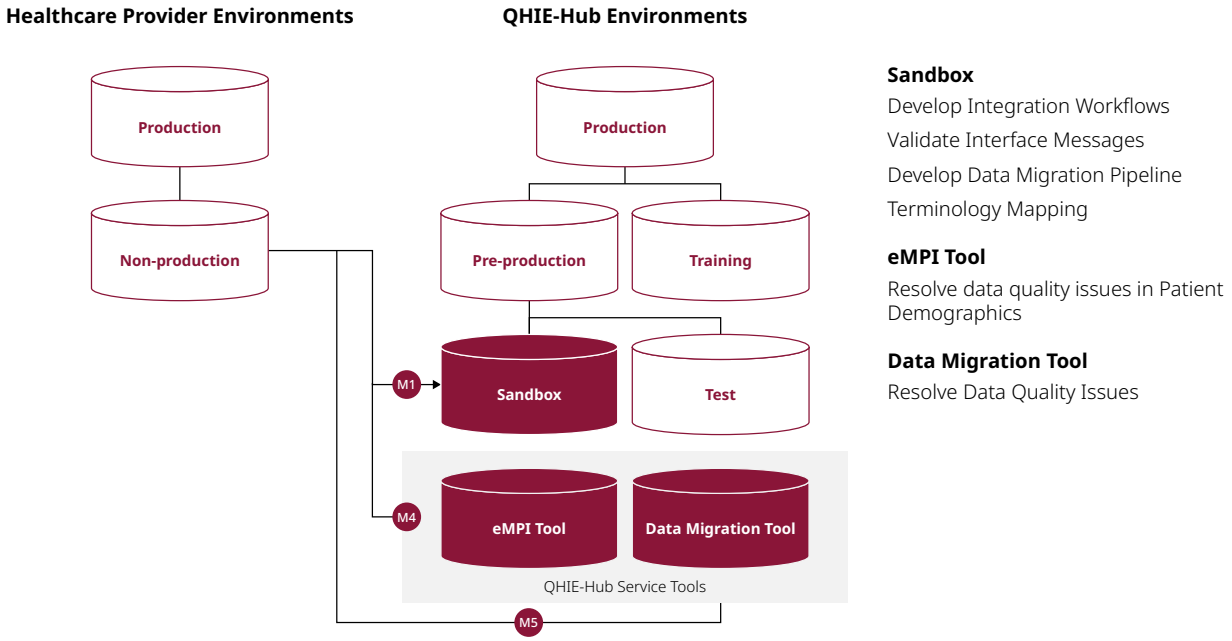


Figure 4. Depiction of Milestones 2, 4 & 5

the healthcare provider can upload CSV files of historical data for all patient resources and get a report on the erroneous clinical records. This tool checks for compliance of the record based on the target data set and business rules for different elements (e.g., a patient's QID is 11 digits, all mandatory fields are available). In this step, healthcare providers must use real data. To complete this step, the healthcare provider should finish the following tasks:

- Assess and resolve all quality issues in real data in their source systems
- Achieve full accuracy in resource data

- **Milestone 6 (Test workflows in Pre-prod):** In this milestone, a healthcare provider must validate interfaces, workflows, and business processes in the Pre-Prod environment before moving to production. After developing and customizing their EMR system in a non-production setting, the provider must obtain approval to connect to the QHIE-Hub's Pre-Prod environment by completing sandbox unit testing and the pre-production assessment from MoPH.This step ensures that all integrations function as expected

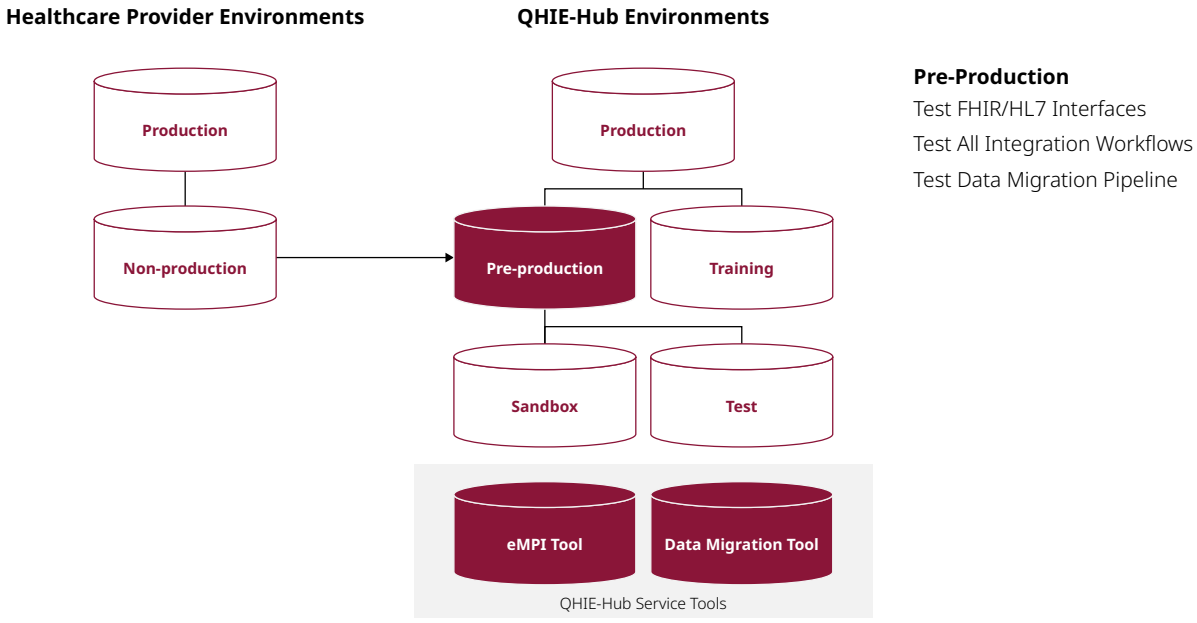


Figure 5. Depiction of Milestones 6

in a simulated environment before live deployment. However, only synthetic data must be used in this step. To cross this milestone, the healthcare provider should successfully finish the following tasks:

  - Obtain approval from MoPH by completing the preproduction assessment
  - Connect to the QHIE-Hub's Pre-Prod environment via the Government Network or ISP Hub
  - Connect with the eConnect/eMeds/ eCare (clinical & health information management teams need to participate in this process)
  - Test all interfaces and integration workflows by using the predefined end to end scenarios and synthetic data (e.g., query, retrieve or create patient records)
  - Test data migration pipelines using synthetic data

- **Milestone 7 (Training):** In parallel to other tasks, healthcare providers should start their training activities. This includes nominating "Train the Trainers" or super-users to attend the trainings organized by MoPH as per the training calendar and then training their end-users through these trainers.
- **Milestone 8 (Onboarding assessment):** Once all the above steps have been completed, the healthcare provider is in a stage where they can proceed to the actual onboarding and integration with the QHIE-Hub's Prod environment. They are required to fill in a Pre-onboarding checklist and seek an Onboarding clearance to connect to the Prod environment of the QHIE-Hub. **This is the second assessment that MoPH will conduct for a healthcare provider.** To meet the requirements of this stage, a healthcare provider must re-verify and confirm that all previous steps have been completed successfully and must submit a report to MoPH.

The onboarding phase starts after all the previous milestones have been achieved and the HCP has received an Approval-to-proceed from MoPH. In this stage, the HCP raises a request to connect their production system to the Prod environment of the QHIE-Hub, migrates historical data and shares a completed user access template.

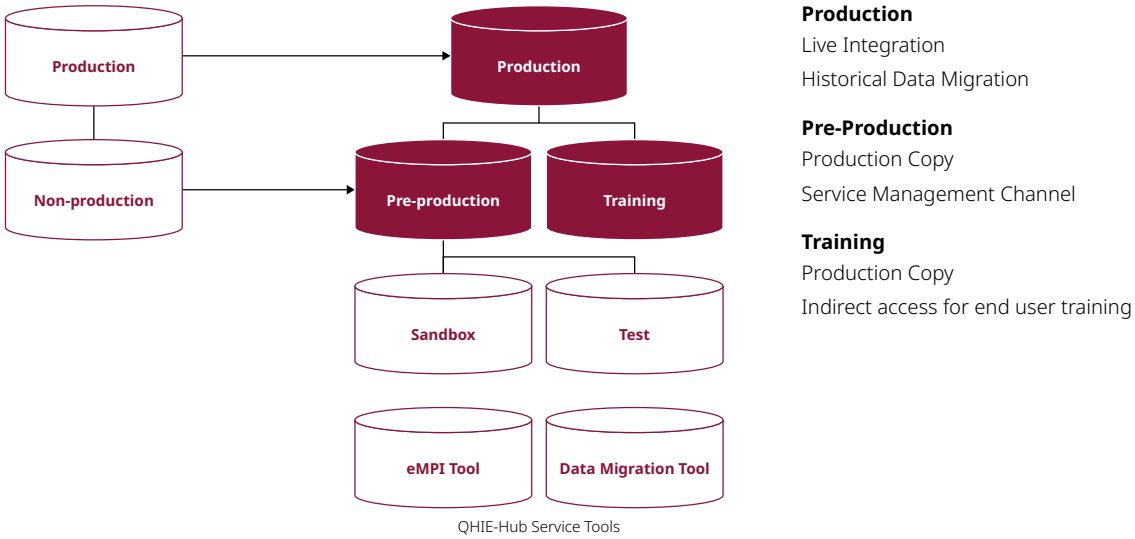


Figure 6. Onboarding and steady state

During Onboarding:

This phase includes the actual onboarding activities after the healthcare provider has received an Onboarding clearance. The pre-requisite for this stage is that the onboarding checklist is filled and all milestones until **Milestone 8** have been completed. There are 2 key milestones healthcare providers need to achieve which are detailed as follows:

- **Milestone 1 (Actual onboarding):** In this step, the actual onboarding starts where the healthcare provider raises a request to connect and integrate their production environment with the QHIE-Hub's Prod environment. This step also involves migration of the historical data to the Prod environment.
  - To ensure a completion of this milestone, a healthcare provider should complete the following tasks:
  - Connect their production environment via GN or the ISP-Hub to the QHIE-Hub's Prod environment
  - Undertake full integration of the Prod environment with the QHIE-Hub Prod environment
  - Completed historical data migration
- **Milestone 2 (Go-live):** This is the final step to complete onboarding of a healthcare provider. In this stage, healthcare providers are required to fill and share the user access template with details about their end-users for bulk-upload and creation in the QHIE-Hub as well as assigning roles to them. Once successful, end-users can start accessing and using the QHIE-Hub services. However, only trained users will be granted access to the national solutions.

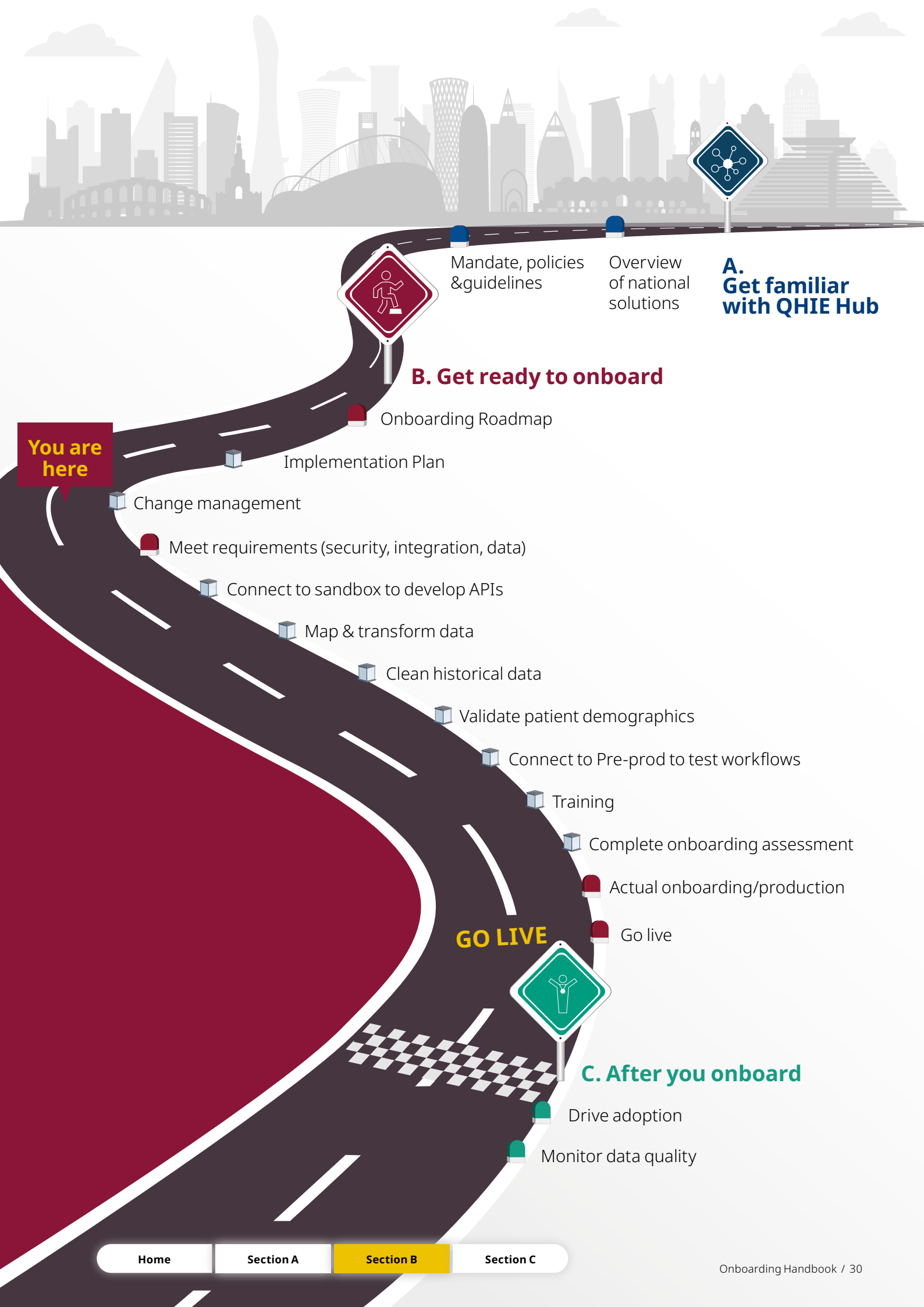
After onboarding:

- After onboarding, healthcare providers must focus on driving 100% adoption within their organization to realize the intended benefits of the QHIE-Hub
- Healthcare providers must prepare and submit a report on adoption metrics and data quality KPIs to MoPH six months after their onboarding. **This will be the third and last onboarding review of a healthcare provider conducted by MoPH**. *(The method, template and frequency of subsequent reviews will be defined by MoPH in due course of time)*
- Healthcare providers must continue to monitor all activities to detect any anomalies, data quality issues or security incidents. If found, they must proactively communicate them to the QHIE-Hub support teams as instructed in the communication plan provided
- Healthcare providers must also continue to stay informed about updates released by MoPH and must install them in their production environment after thorough planning, implementing and testing in their non-production environment.

4.2 Pre-Onboarding Assessment

As outlined in the onboarding journey above, a healthcare provider must conduct a gap analysis to determine their readiness before they start their onboarding journey to identify areas for transformation. These results will determine initiatives that need to be undertaken as part of the change management. A detailed implementation plan for this stage is shared with the rest of the onboarding resources.

*****


Mandate, policies &guidelines
Overview of national solutions
A. Get familiar with QHIE Hub
B. Get ready to onboard
Onboarding Roadmap
You are here
Implementation Plan
Change management
Meet requirements (security, integration, data)
Connect to sandbox to develop APIs
Map & transform data
Clean historical data
Validate patient demographics
Connect to Pre-prod to test workflows
Training
Complete onboarding assessment
Actual onboarding/production
GO LIVE
Go live
C. After you onboard
Drive adoption
Monitor data quality

CHAPTER 5

People & Support

This chapter provides an overview of change and communication-related aspects as part of a healthcare provider's onboarding journey. It covers the change management toolkit, communication channels to be used by MoPH and other resources that healthcare providers can expect throughout their journey.

5.1 Change management toolkit

To ensure a successful onboarding to the QHIE-Hub, it is essential for healthcare providers to develop a change management strategy for all stakeholders and processes that are likely to be impacted by the technological change (based on gaps identified in the earlier phases of onboarding). The objective of this section is to provide an approach to develop a change management strategy and an implementation plan to operationalize it.

Change management, in the context of the QHIE-Hub, is defined as the process of dealing with the transformation or transition of day-to-day processes or systems. This includes changes in both technical and business workflows that impact end-users. A robust change management strategy aims to:

- Implement strategies and initiatives to ensure change is rolled out and effective
- Communicate the changes to stakeholders
- Help stakeholders understand and adopt to the changes

For a smooth onboarding process, it is essential for healthcare providers to develop a change management team which undertakes the transformation initiatives to meet the requirements of the QHIE-Hub.

There are four best practices that determine the success of change management. Healthcare providers are advised to consider these when defining their change management strategy:

1. Secure buy-in from key stakeholders and drive top-down messaging
2. Ensure change management is centrally-led and monitored (i.e., via a change management team)
3. Embed key activities and initiatives into an actionable plan with clear initiative owners
4. Adopt an agile approach to implement changes and to course-correct after regular evaluation
5. Monitor the milestones and hold owners of the milestones accountable

It is recommended that healthcare providers follow a 3-step process to change management as outlined in the figure 7.

Figure 7. Steps involved in change management

5.1.1 Recommended team structure

A change management team typically comprises of three profiles. Each provider is advised to identify these profiles in their respective organization and to set up a change management team. Team size may vary based on the size of the organization.

No.	Roles	Responsibilities
1	**Change management lead**	• Oversee the change management team and develop stakeholder engagement plans • Review the status of the change management effort on a regular basis and course-correct the plan as needed • Provide updates on the plan to the senior management
2	**Change management team member**	• Develop and execute enterprise-wide initiatives • Monitor performance against established KPIs • Develop relevant delivery management tools, templates, and solutions
3	**Change management coach**	• Support initiative owners in developing and / or executing their initiatives • Ensure compliance to methodologies and tools established by the central change management team • Ensure proper document management of change management initiatives • Communicate the key messages from the change management team to initiative owners • Help escalate bottlenecks raised by initiative owners to the central team and address the issues

Table 2. Roles and responsibilities within change management teams

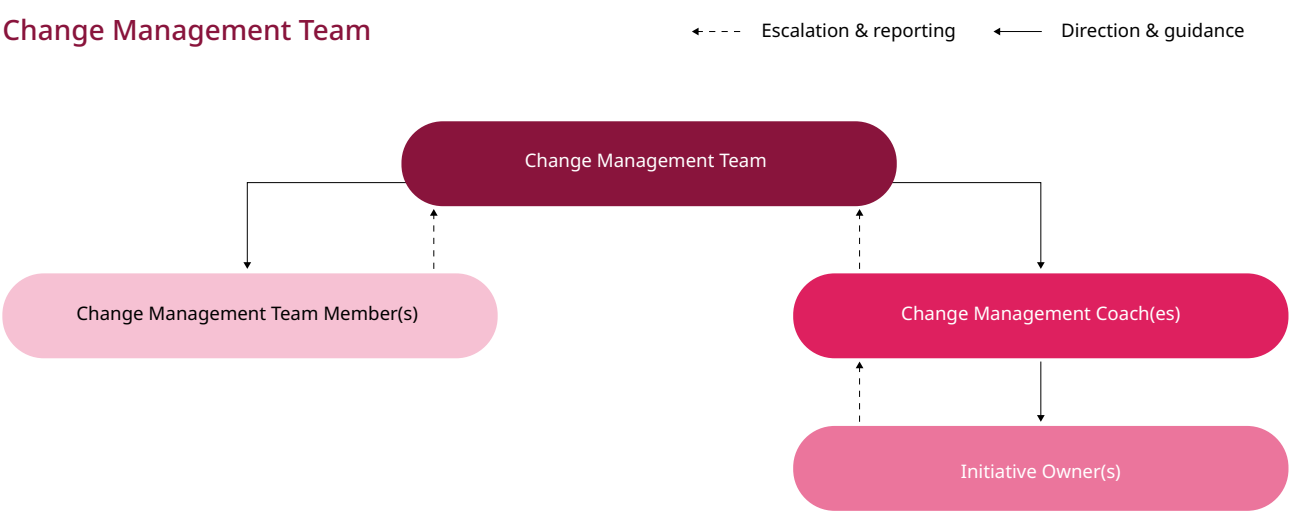


Figure 8. Change management team structure

Initiative name

Description A high-level overview of what the initiative is and the intended impact it aims to achieve

Objective A description of the initiative goals

Quantitative initiative targets (following SMART criteria i.e., specific, measurable, actionable, relevant and time-bound

Key stakeholders A list of stakeholders the initiative will target

A list of the key decision makers

Owner

Name of individual or department that will be responsible for executing the initiative

Project Milestones	Timing (Due Date)
1. Description of key activities	DD-MM-YY
2. Description of key activities	DD-MM-YY
3. Description of key activities	DD-MM-YY
4. Description of key activities	DD-MM-YY
5. Description of key activities	DD-MM-YY

Figure 8.1. Initiative Charter Template

5.1.2 Diagnose change readiness & design initiatives

Based on the results of the pre-onboarding assessment, healthcare providers are advised to determine their current state across technical requirements and identify gaps. Once gaps are identified, providers can develop a list of initiatives to address these gaps. For each gap, an initiative charter needs to be developed with the objective, initiative owner(s), key stakeholders, key milestones, and the respective due dates.

There can be two types of initiatives:

1. Enterprise-wide (e.g., announcement of roll-out of national solutions across the organization, training for healthcare practitioners)
2. Function-specific (e.g., developing target datasets)

The enterprise-wide initiatives can be led by the change management team, while the function-specific initiatives can be led by initiative owners from different parts of the organization (who are guided and supported by the central team).

5.1.3 Set up a governance cadence

The change management team is responsible for ensuring all change initiatives are implemented as per the defined plan and timelines. For this, it needs to monitor progress on the plan at a frequent basis (e.g., weekly) and raise any issues, risks or challenges that may affect the plan to the senior management.

Therefore, it is recommended that a governance cadence is developed to ensure operationalization of the change management initiatives. This could include:

- Monthly steering committee discussions with senior management
- Fortnightly progress update meetings for initiatives led by the change management lead
- Weekly check-ins with change management coach and initiative owner to outline priorities of the week
- Other working group meetings as required

Governance cadence to monitor status is necessary to ensure all change initiatives are implemented as per the defined plans and timelines. It also enables timely escalation of issues and their resolution.

It is important to note that communication with all stakeholders is essential in the process of identifying, planning, and implementing a successful change management plan. Ensuring that all members have clear and open lines of

communication throughout the process is also essential to drive outcomes. Healthcare providers must establish transparency and two-way communication systems that allow members to raise their issues and seek help.

5.1.4 MoPH support throughout your journey

The Ministry of Public Health will provide comprehensive support to healthcare providers across all stages of their onboarding to the QHIE-Hub. The primary objective is to aid the transformation of healthcare providers, ensure a seamless integration with the QHIE-Hub and to drive solution adoption across end-users.

5.1.4.1 Support in the pre-onboarding phase

1. **Share self-help resources** : Exhaustive resources as outlined in the document hierarchy (e.g., policies, interface specifications, templates, data sets etc.) will be published for all healthcare providers across solutions via Exchange Medium and Onboarding Portal. These will serve as guides on all technical topics (e.g., data, connectivity, integration, identity management and security) and business workflow changes. These will also include solution and entity-specific topics where further guidance is needed. The overall imperative is to enable healthcare providers to get well-acquainted with the requirements of the QHIE-Hub solutions and to facilitate smooth onboarding. Exchange Medium is available.
2. **Conduct townhalls and open days** : MoPH teams will conduct periodic townhall sessions to create awareness and address points of concerns for healthcare providers. These town halls will be virtual / hybrid.

   For additional pre-onboarding support, there will be calendarized open days conducted by MoPH to familiarize healthcare providers with specific topics, address queries, and extend relevant preparatory support for onboarding. Frequently asked questions from healthcare providers and their answers will be published on the Onboarding portal for ready reference.

5.1.4.2 Support during the onboarding phase

1. **Assign a facility manager from the onboarding task force** : MoPH has set up an onboarding task force that will act as a nodal agency for the overall rollout and onboarding process. Each facility will be assigned a facility manager as point of contact from this team via an official email from MoPH. The facility manager will be the first point of contact from MoPH during the onboarding journey of a healthcare provider. They will also serve as a point of functional and hierarchical escalation for the respective healthcare provider.

   The facility manager will help healthcare providers to:

   - Get destination URLs to establish connectivity with the QHIE-Hub
   - Raise internal tickets to approve connectivity requests
   - Help in systems identities creation once healthcare providers share the completed form
   - Schedule the testing window for healthcare providers to test their developed APIs in sandbox environment and their workflows in defined slots using synthetic data in the pre-production environment
   - Confirm the success of test cases in the pre-production environment
   - Secure “Onboarding clearance” based on completion status of the onboarding checklist assessment for preproduction, production and go live
   - Ensure that the historical data migration API has been tested and is ready or share the INPUT SAS URLs for the data migration tool (if approval is granted for the CSV-based data migration approach, ensure the necessary files are prepared and shared accordingly)
   - Support bulk-upload and creation of users after production connectivity is established
2. **Plan and schedule Train-the-trainer training programs** : When healthcare providers are ready for onboarding, MoPH will request nominations for train-the-trainer programs and extend an invitation

to nominated trainers / super users. These trainees will be responsible for training end-users within their organization. A detailed training calendar will be published for all healthcare providers. Additionally, training materials, environments, and comprehensive training guides for nominated trainer / super-users will be available for all solutions.

5.1.4.3 Support post onboarding

1. **Provide support and maintenance** : MoPH will provide two channels that healthcare providers can utilize for continuous support. A centralized telephone helpline **(+974 5107 8116)** is the primary channel that can be used for standard and critical incidents. Healthcare providers can also email **[nationalhealthplatform@moph.gov.qa]** to raise support tickets or report issues. If an issue is not resolved within the specified resolution time or requires further attention, it can be escalated using the same email id. (Facility managers can be added to these escalations only before and during onboarding. They will be unavailable after Go-live).

   Additional details are available in Chapter 9.3 Leverage support & maintenance

5.1.5 Communication channels

Timely communication is a critical success factor to inform healthcare providers about key program updates and to share information about the QHIE-Hub. The communication team at MoPH aims to streamline all program related communication to specific channels to ensure healthcare providers do not miss any important information. This section provides additional details about the primary communication channels that will be leveraged by MoPH.

Additional details are available in Communication Plan for healthcare provider.

1. **Designated email**: Email is a preferred communication channel for all program-related activities. All healthcare providers will receive designated email ids for support. These can be leveraged by healthcare providers to send requests and and to seek additional information.
2. **QHIE-Hub website:** The QHIE-Hub website is an information portal dedicated to the QHIE-Hub program and consists of information on all the national solutions. Important links to program related news, announcements, training schedules and links to training and onboarding resources will be available on the website.
3. **Onboarding portal:** The Onboarding Portal will serve as the primary source of onboarding-related information, replacing the existing exchange medium. It will provide a centralized repository for essential resources, including the onboarding handbook, templates, guides, and a comprehensive list of FAQs. Focal points from a healthcare provider's organization will be provided login credentials to access this material (e.g., training documents, manuals, self-learning videos etc.) and to track completion of activities across onboarding milestones using digital checklists. The portal will also be used to conduct periodic reviews and assessments of the healthcare provider before, during and after their onboarding to the QHIE-Hub.

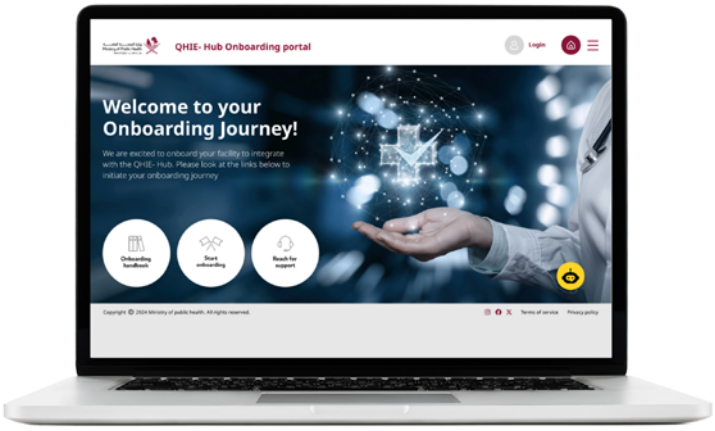


Figure 9. Self-help resources provided by MoPH

CHAPTER 6

Meet the Requirements

6.1 Security & connectivity

This section outlines key cybersecurity and network connectivity requirements for healthcare providers integrating with the QHIE-Hub, ensuring compliance with Qatar's National Information Assurance Policy (NIAP) and Data Protection Law (DPL 2016). These requirements are structured across three core pillars: Infrastructure security, Privacy protection, and Connectivity standards.

Before a healthcare provider raises a request to establish a connection with QHIE-Hub, they must meet all cybersecurity requirements. These will be evaluated by MoPH before approving the request.

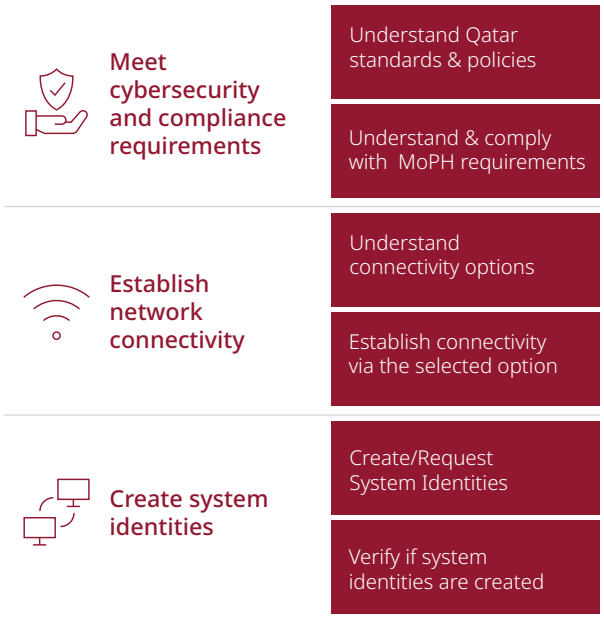


Figure 10. High-level infrastructure and connectivity roadmap for healthcare providers

6.1.1 Cybersecurity

Given that Protected Health Information (PHI) and Personally Identifiable Information (PII) will be exchanged through the QHIE-Hub, safeguarding data confidentiality, integrity, and availability is a top priority. All medical data is classified under C3 confidentiality, with specialized controls for VVIP records and sensitive data, protected with enhanced security controls.

To comply with these standards, healthcare providers must implement and maintain Zero Trust Architecture (ZTA), multi-layered encryption, and AI-driven threat detection while maintaining a need-to-know access control policy. The following security protocols ensure compliance with Privacy by Design principles and QHIE-Hub security policies.

6.1.1.1 QHIE-Hub cybersecurity requirements

All healthcare providers are required to implement the below list of privacy and security protocols:

- Healthcare providers must connect to the QHIE-Hub only through the Health Connect network (Government Network, and Ooredoo and Vodafone private networks) (detailed in this section).
- Healthcare providers must ensure that all endpoints and middleware connecting to the QHIE-Hub have antivirus/antimalware installed that is up to date.
- Healthcare providers need to ensure that all endpoints and middleware connecting to the QHIE-Hub have the latest security patches applied; furthermore, these endpoints & middleware accessing the QHIE-Hub are not allowed to access the internet.
- Healthcare providers are required to ensure that connecting external storage to endpoints and middleware accessing the QHIE-Hub is prohibited.

- Healthcare providers must use only FHIR API, or HL7v2 API (supported temporarily until December 2025), for integration with QHIE-Hub
- Healthcare providers are required to make sure all PII and PHI is shared over a secure electronic network, and all information in transit and at rest is encrypted to prevent unauthorized access.
- Healthcare providers must ensure that data encryption is done both at rest and in-transit for all PII and PHI data processed or stored by them.
- Only trained authorized healthcare professionals, members of the care teams and administrators (authorized users) should be given access to the QHIE-Hub. Healthcare providers are required to assign role-based access permissions using the HIM (Health Information Management) Portal of the QHIE-Hub, which are need-to-know, need-to-have basis only (will be reinforced by the national solutions in the QHIE-Hub).
- Healthcare providers are required to protect their network and endpoint by appropriate security controls (e.g., endpoint security, network security, physical security, remote access security, vulnerability and patch management, threat detection and prevention).
- Healthcare providers must implement data classification and labeling aligned with NIA Policy along with necessary data protection and data loss/leakage prevention controls.
- Healthcare providers are required to have enhanced access control on the server used for data Integration with the QHIE-Hub (e.g., multi-factor authentication and password strength requirement)
- Healthcare providers must have controls to enforce approved authorizations for controlling the flow of information within their system, and between connected systems.
- Healthcare providers are required to maintain audit logs of all PII and PHI modifications and share records of changes with the QHIE-Hub as per compliance requirements.
- Healthcare providers must ensure third-party services are controlled through suitable procedural obligations and contractual terms to secure privacy and protect PII and PHI assets.
- Healthcare providers must ensure that systems accessing the QHIE-Hub are strictly isolated from internet access to prevent unauthorized external exposure.
- Healthcare providers must prohibit Node-to-Node direct communication between systems accessing the QHIE-Hub and ensure all communication occurs over secure ports only.
- Healthcare providers must ensure that vendor connections to the local network specify a real IP address, cannot use a subnet, and can only connect to an allowed IP range.
- Healthcare providers must configure their DNS with conditional forwarding of only the QHIE-Hub FQDNs to 172.30.230.196 as per QHIE-Hub network requirements.
- Healthcare providers must implement encryption key lifecycle management, ensuring keys have a defined lifetime and are immediately revoked and replaced if compromised.

All HCPs need to connect to the QHIE-Hub via the Health Connect that has two different methods – the Government Network Hub for Public HCPs and ISP Hubs for Private HCPs.

- Healthcare providers must ensure that sensitive data in databases classified as C3 and above is masked using data masking technology to prevent unauthorized exposure.
- Healthcare providers must ensure that only supported operating systems are used, and any end-of-support OS versions, including Windows Server 2012 and Linux 6, are strictly prohibited.
- Healthcare providers must disable USB ports on all endpoints accessing the QHIE-Hub to prevent unauthorized data extraction and security breaches.

- Healthcare providers must ensure that all unused software is uninstalled, and all software and security patches remain up to date to mitigate vulnerabilities.
- Healthcare providers must disable all unused ports and services to minimize exposure to cybersecurity threats.

viewer (eConnect) and the ePrescription and Digital Pharmacy (eMeds), and Registries and Care plans (eCare)).

There are 2 main steps in this process as outlined in the Figure 11.

Figure 11. Steps to connect with the QHIE-Hub

- Healthcare providers must ensure that automatic session timeout is enabled to prevent unauthorized access from unattended systems.
- Healthcare providers must ensure that logging mechanisms capture system access, transmission, security events, and processing activities, including date, time, authentication activity, failure logs, change actions, and command outputs.
- Healthcare providers must ensure that they implement and maintain a Security information and event management (SIEM) technology which supports threat detection, compliance and security incident management through the collection and analysis (both near real time and historical) of security events, as well as a wide variety of other event and contextual data sources, any that all identified security incidents or suspicious activities are reported immediately to the designated security authorities.

6.1.2 Network connectivity

This section explains connectivity processes for healthcare providers to connect with the QHIE-Hub and the national solutions.

As part of onboarding, healthcare providers must connect with four environments. These include the sandbox environment (to validate their API messages), the Training environment (to train end users on the solutions), Pre-Prod environment (to test APIs and business processes) and the Prod environment (during go-live). These connections must be made for every solution that they need to get onboarded to (i.e., the National Health Information Platform (QHIE-Hub), National clinical

Depending on the type of facility, one of the below methods within the Health Connect network are required to be utilized in each approved Healthcare Provider network, to connect to the QHIE-Hub. This method is fixed for all subsequent connections with not only the QHIE-Hub, but all MOPH National Solutions (including the Qatar National Health Insurance Solution). There will be no connectivity for Healthcare Providers over the Internet.

1. Public Healthcare Providers (government and semi-government) should use the Government Network Hub
2. Private Healthcare Providers should use their local ISPs (ISP Hub) via Ooredoo or Vodafone

The conceptual diagram (*Figure 12)* explains how healthcare providers can connect using the available options.

6.1.2.1 Network connectivity via Government Network (GN) Azure Hub

The Government Network Azure Hub (GN Azure Hub) supplies connectivity between government and semi-government agencies. Hence, Public Healthcare Providers that are already connected via the GN Azure Hub can leverage their existing connection to connect with the QHIE-Hub and other national solutions like the Qatar National Health Insurance Solution. The below process needs to be followed to connect to the QHIE-Hub via GN Azure Hub:

1. Healthcare provider should initiate a GN Request with the required Source IP addresses to map to the MOPH Destination IP address for each environment (Sandbox, Pre-Production, Production, Training) and National Solution and share details about their environment

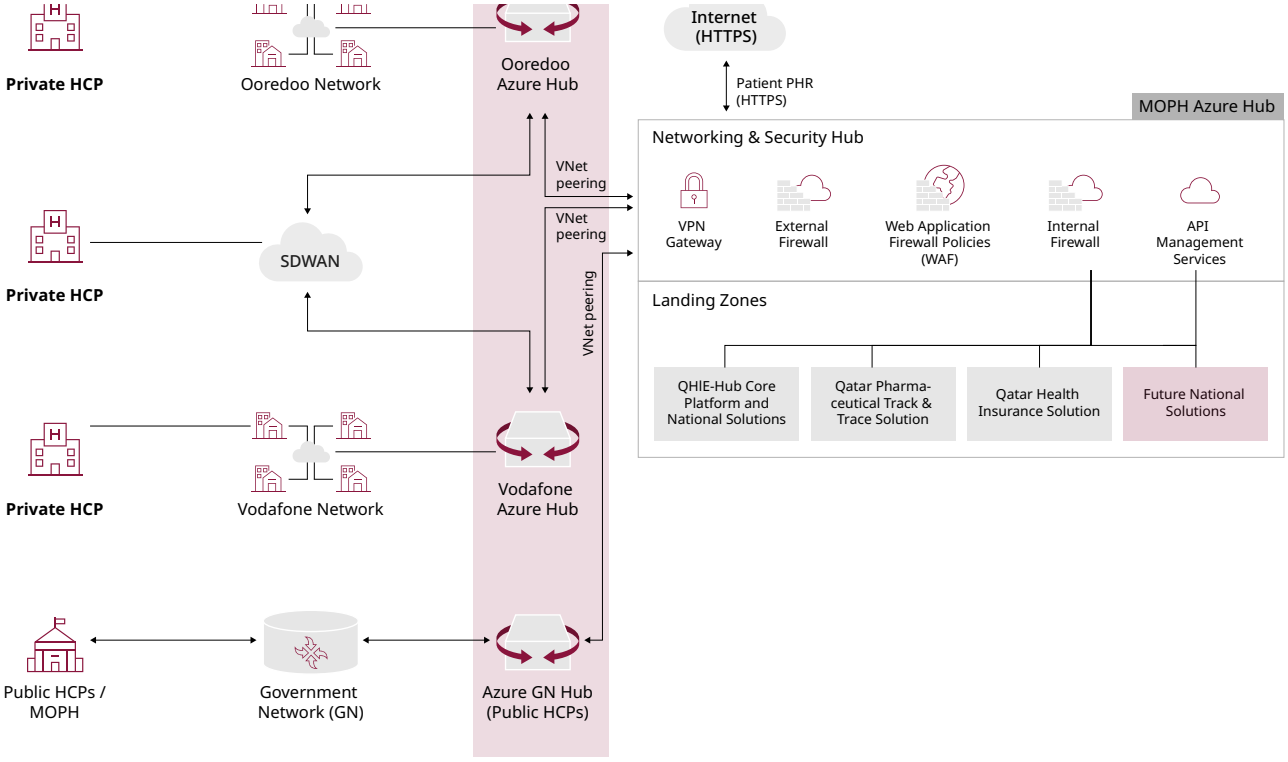


Figure 12. Connectivity options available to healthcare providers

and the purpose of connectivity using the **Connectivity Request Template** available with the onboarding handbook .

2. All parties need to jointly agree on the network matrix details such as source and destination IP addresses, ports, and URLs.
3. The healthcare provider network team should request the GN team for the latest version of the connectivity form and raise a change request with them (ensuring to request connection to site "MOPH-Azure"). Furthermore, they should also submit a

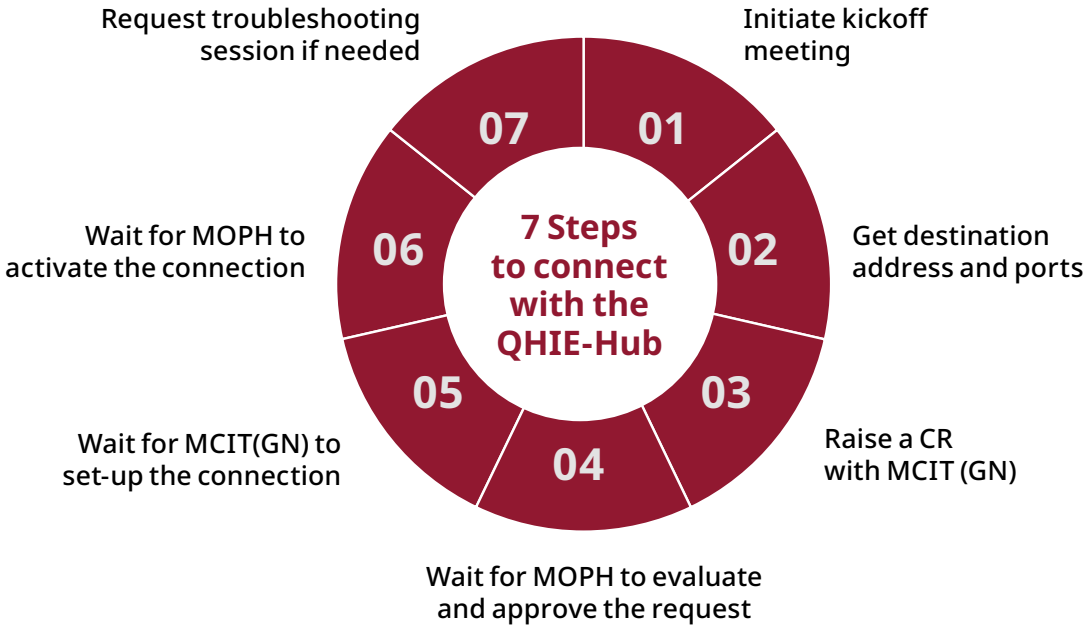


Figure 13. Steps to connect with the QHIE-Hub

completed MoPH Security Compliance Checklist with their request.

4. GN will then raise an approval request to MoPH.
5. MoPH will evaluate the request along with the information in the MoPH Security Compliance Checklist and may request more information before approval.
6. Once approved by MoPH, GN will set up the connectivity.
7. MoPH will activate the connection from its side according to the details received from the Healthcare Provider in the Connectivity Template.
8. Healthcare providers can request a session to verify the connection and troubleshoot any issues.

HCPs need to contact their prefered provider to understand their process and requirements to connect to QHIE's hub.

6.1.2.2 Connectivity via the ISP Hub

MoPH has worked with major ISPs (Ooredoo and Vodafone) to establish the ISP Hub. Private healthcare providers can use this method to connect to the QHIE-Hub, its national solutions, and other national solutions like Qatar National Health Insurance Solution. To connect to MoPH via the ISP Hub, the healthcare provider should follow the below process.

1. Healthcare providers need to contact their preferred ISP (Ooredoo or Vodafone) and enter into a contract to install the requisite network devices (and potentially network links) to connect to the QHIE-Hub via the ISP Hub. Furthermore, they should also submit a completed Connectivity Template (with the MoPH Security Compliance Checklist) available with the onboarding handbook as part of their request.
2. The ISP will guide the healthcare provider on the plans/services and agreements they need to sign and on any equipment that the healthcare provider may need to obtain.
3. Once healthcare provider is ready, the ISP will then raise an approval request with MoPH.
4. MoPH will evaluate the request and may request more information before approval.
5. Once approved by MoPH, the ISP will set up the connectivity for the healthcare provider.
6. MoPH will activate the connection from its side according to the details received from Healthcare Provider in the Connectivity Template.
7. Healthcare providers can request a session to verify the connection and troubleshoot any issues (see HCP Connectivity Guide for troubleshooting steps).

Note: Destination URLs (FQDNs) are provided in the Connectivity Template matrix.

6.1.2.3 Create system identities

This section outlines the process of creating system identities for API Clients (API credentials) that are required for system-to-system integration. To consume any API that is provided by the QHIE-Hub, an API client registration within QHIE-Hub is required. An API Client will have the following properties:

- *Client ID*
- *Application Type such as EMR, LIS, RIS*

Figure 14. Steps to connect via ISP Azure Hub

- *Client Name*
- *Contact Phone Number and e-mail.*
- *Source of client e.g. Healthcare Provider, Ministry Entity*
- *Client Facility*
- *Client Credentials*
- *Roles*

The QHIE-Hub Supports three types of client credentials:

- *APIM Subscription Key*
- *Client Secret*
- *Client ID*

The OAuth 2 client-credentials authentication method will be used for system-to-system integrations. The client systems that need to access QHIE-Hub API services will have to register in the Identity Service.

The registration and configuration of client/ consumer systems (e.g., EMR, LIS, RIS) will be managed by MoPH admin users. A healthcare provider can have more than one registered client system. However, each client will have its client credentials, and they can use this credential information to retrieve access tokens. Based on the environments outlined in the onboarding roadmap, healthcare providers are required to use generated credentials for every environment that they connect to.

To create system identities and generate client credentials, healthcare providers need to follow the below process:

1. Healthcare Provider needs to fill the **Systems Identities Creation form** and inform MoPH
2. MoPH will evaluate the request based on the provided information and may request additional details if needed before granting approval
3. MoPH will implement client registration within QHIE and provide the HCP Client ID, Client Secret, and APIM subscription key through a secure channel

The healthcare provider's IT team must follow the steps outlined by MoPH in the HCP Connectivity Guide to enable their systems using the provided credentials

6.2 Integration

The QHIE-Hub is envisioned to be a central as well as federated platform – a patient centric repository for exchanging and storing the longitudinal patient journey, enhancing cross provider communication. It will provide an Enterprise Service Bus that all stakeholders of the healthcare ecosystem in Qatar can utilize to exchange health information in a way which not only transmits data in electronic format but also ensures compliance and standardization of the data passing through the QHIE-Hub.

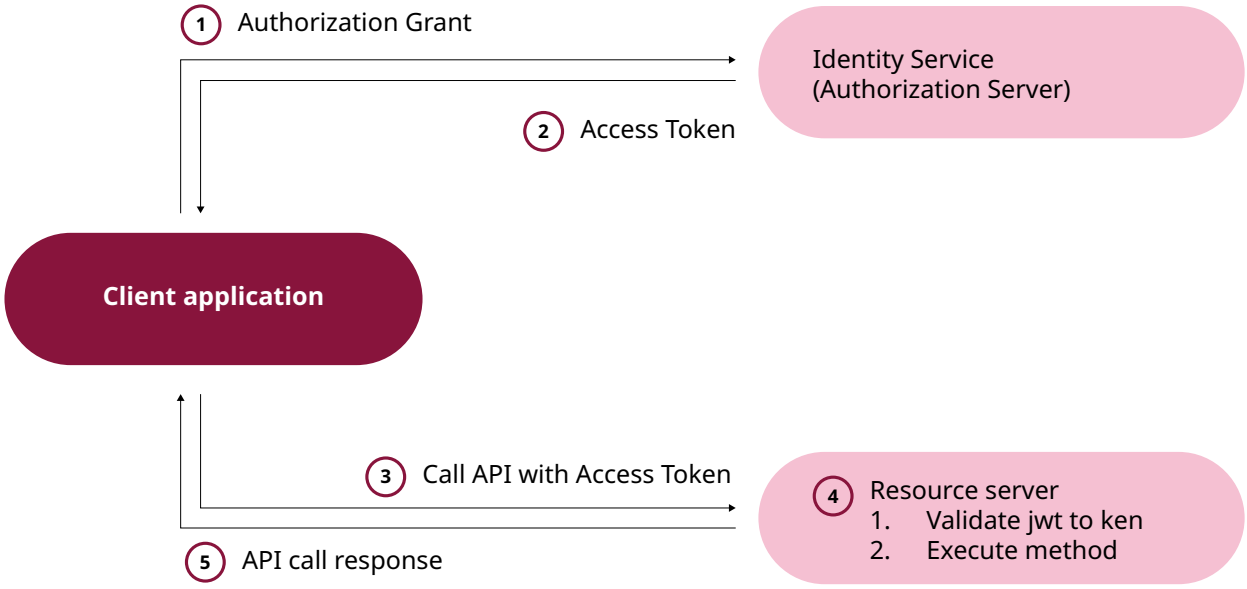


Figure 15. OAuth 2 client-credentials flow

Integration with the QHIE-Hub has four steps as depicted in the figure 16.

6.2.1 Review supported standards & integration specifications

The QHIE-Hub follows the secure protocol for data transmission (https). All healthcare providers need to configure their systems to send and receive these messages securely. The overall system has been designed to support international integration standards to exchange data between systems (where appropriate). Those standards are as follows:

1. **FHIR R4B:** FHIR (Fast Healthcare Interoperability Resources) is essentially an application programming interface (API)-focused standard used to represent and exchange health information maintained by the standards development organization, HL7®
   As part of the QHIE-Hub program, MoPH has profiled certain resources and data elements to meet the healthcare workflows / practices and constraints in the State of Qatar. Detailed specifications can be found in the Interface specifications for FHIR, shared as part of the onboarding resources.
2. **HL7 v2.5.1:** HL7 (Health Level 7) is a set of clinical standards and messaging formats that provide a framework for the management, integration, exchange, and retrieval of electronic information across different healthcare systems.
   Detailed specifications can be found in the Interface specifications for HL7 v2.5.1, shared as part of the onboarding resources.

A client id and secret key are mandatory to authorize the sending system/facility by creating a JWT token that is subsequently used for exchanging data with the QHIE-Hub. HL7 (Health Level 7) integration is supported only until December 2025. All facilities must transition to FHIR, as MoPH projects standardize on FHIR. HL7 v2 support is temporary and will be discontinued.

Two standard messaging formats are used for exchanging clinical information between the QHIE-Hub and HCPs: FHIR and temporarily HL7 v2.

6.2.2 Understand data APIs

This section details the description, resources, and events for FHIR and HL7 V2.5.1. Further details are available in the Interface specification documents for both standards provided by MoPH.

6.2.2.1 FHIR 4B

FHIR is described as a 'RESTful' specification based on common industry-level use of the term REST (Representational State Transfer). The FHIR API Server within the QHIE-Hub implements the **HL7 FHIR HTTP API** and supports the set of FHIR-defined resource types.

FHIR APIs will be used to manage the QHIE-Hub FHIR profiles. A profile is an entity that has a known identity, contains structured data, and has a version number. The structure of each profile is shared in the Target data set provided by MoPH. The following FHIR profiles are considered in the QHIE-Hub:

The latest and up-to-date FHIR resources utilized within the QHIE-Hub are detailed in the integration specifications document and other relevant integration documents. Refer to these documents to stay informed about any changes.

6.2.2.2 HL7 V2.5.1

This messaging standard will be supported temporarily until December 2025. It allows the exchange of clinical data between systems and is designed to support a central patient care system as well as a distributed environment where data resides in departmental systems. HL7 v2 messages should be used in a messaging context when the healthcare provider does not

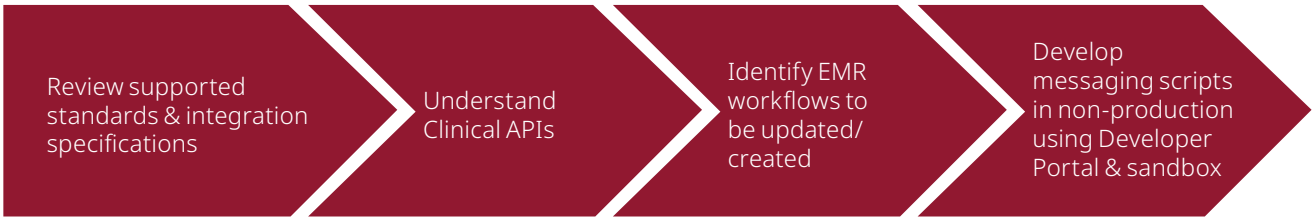


Figure 16. Steps to integrate with the QHIE-Hub

have the capability to send FHIR messages. The version adopted by the QHIE-Hub is 2.5.1.

Since all clinical data in the QHIE-Hub is managed in the FHIR format, HL7 messages will be transformed before they are sent to the QHIE-Hub's FHIR server. Healthcare providers should expect an ACK response if the message is processed successfully. If the validation in the QHIE-Hub FHIR server fails, NACK response will be returned with validation errors.

The data flow is outlined in Figure 18.

The selected transport layer protocol for HL7 messages in the QHIE-Hub is HL7 over HTTPS. This mechanism uses the Hypertext Transfer Protocol (as defined in RFC 2616) to transmit HL7 artifacts (such as messages, documents, resources).

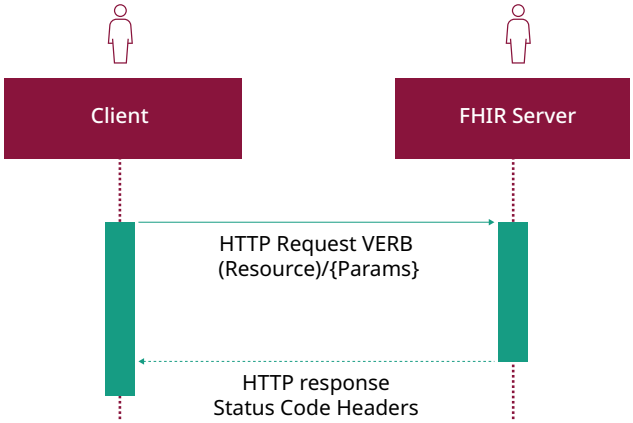


Figure 17. Client-server communication in FHIR

The following message events are considered in the QHIE-Hub:

#	Resource name	Description
1	Encounter	An interaction between a patient and healthcare provider(s) for the purpose of providing healthcare service(s) or assessing the health status of a patient.
2	Condition	A clinical condition, problem, diagnosis, or other event, situation, issue, or clinical concept that has risen to a level of concern.
3	Observation	Measurements and simple assertions made about a patient, device, or other subject.
4	CarePlan	Describes the intention of how one or more practitioners intend to deliver care for a particular patient, group, or community for a period, possibly limited to care for a specific condition or set of conditions.
5	DiagnosticReport	The findings and interpretation of diagnostic tests performed on patients, groups of patients, devices, and locations, and/or specimens derived from these. The report includes clinical context such as requesting and provider information, and some mix of atomic results, images, textual and coded interpretations, and formatted representation of diagnostic reports.
6	DocumentReference	A reference to a document of any kind for any purpose that provides metadata about the document so that the document can be discovered and managed. The scope of a document is any serialized object with a mime-type, so includes formal patient centric documents (CDA), clinical notes, scanned paper, and non-patient specific documents like policy text.
7	Immunization	Describes the event of a patient being administered a vaccine or a record of an immunization as reported by a patient, a clinician, or another party.
8	FamilyMember History	Significant health conditions for a person related to the patient relevant in the context of care for the patient.
9	Procedure	An action that is or was performed on or for a patient. This can be a physical intervention like an operation, or less invasive like long term services, counselling, or hypnotherapy.
10	Goal	Describes the intended objective(s) for a patient, group, or organization care. For example, weight loss, restoring an activity of daily living, obtaining herd immunity via immunization, meeting a process improvement objective, etc.

Table 3. FHIR profiles (continued...)

#	Resource name	Description
11	CareTeam	The Care Team includes all the people and organizations who plan to participate in the coordination and delivery of care for a patient.
12	AllergyIntolerance	Risk of harmful or undesirable, physiological response which is unique to an individual and associated with exposure to a substance.
13	Related Person	Information about a person that is involved in the care of a patient, but who is not the target of healthcare, nor has a formal responsibility in the care process.
14	Communication Request	A request to convey information (e.g., the CDS system proposes that an alert be sent to a responsible provider or proposes that the public health agency be notified about a reportable condition).
15	Service Request	A record of a request for service such as diagnostic investigations, treatments, or operations to be performed.
16	Medication Administration	Describes the event of a patient consuming or otherwise being administered a medication. This may be as simple as swallowing a tablet or it may be a long running infusion. Related resources tie this event to the authorizing prescription, and the specific encounter between patient and health care practitioner.
17	Patient	Demographics and other administrative information about an individual or animal receiving care or other health-related services.
18	Medication Request	An order or request for both supply of the medication and the instructions for administration of the medication to a patient. The resource is called "MedicationRequest" rather than "MedicationPrescription" or "MedicationOrder" to generalize the use across inpatient and outpatient settings, including care plans, etc., and to harmonize with workflow patterns.
19	Medication Dispense	Indicates that a medication product is to be or has been dispensed for a named person/patient. This includes a description of the medication product (supply) provided and the instructions for administering the medication. The medication dispense is the result of a pharmacy system responding to a medication request.
20	Medication Statement	A record of a medication that is being consumed by a patient. A MedicationStatement may indicate that the patient may be taking the medication now or has taken the medication in the past or will be taking the medication in the future. The source of this information can be the patient, significant other (such as a family member or spouse), or a clinician. A common scenario where this information is captured is during the history taking process during a patient visit or stay. The medication information may come from sources such as the patient's memory, from a prescription bottle, or from a list of medications the patient, clinician or other party maintains.
21	EpisodeOfCare	An association between a patient and an organization / healthcare provider(s) during which time encounters may occur. The managing organization assumes a level of responsibility for the patient during this time.
22	NutritionOrder	A request to supply a diet, formula feeding (enteral) or oral nutritional supplement to a patient/resident.
23	RiskAssessment	An assessment of the likely outcome(s) for a patient or other subject as well as the likelihood of each outcome
24	Account	A financial tool for tracking value accrued for a particular purpose. In the healthcare field, used to track charges for a patient, cost centers, etc.
25	Appointment	A booking of a healthcare event among patient(s), practitioner(s), related person(s) and/or device(s) for a specific date/time. This may result in one or more Encounter(s).

Table 3. FHIR profiles (continued...)

#	Resource name	Description
26	Location	Details and position information for a physical place where services are provided and resources and participants may be stored, found, contained, or accommodated.
27	Questionnaire	A structured set of questions intended to guide the collection of answers from end-users. Questionnaires provide detailed control over order, presentation, phraseology and grouping to allow coherent, consistent data collection.
28	Questionnaire-Response	A structured set of questions and their answers. The questions are ordered and grouped into coherent subsets, corresponding to the structure of the grouping of the questionnaire being responded to.
29	Medication	This resource is primarily used for the identification and definition of a medication for the purposes of prescribing, dispensing, and administering medication as well as for making statements about medication use.
30	Communication	The purpose of a communication resource is to surface that data was shared to track adherence to guidelines or protocols or to provide business documentation of actions taken.
31	Composition	The Composition resource defines a set of healthcare-related information that is assembled into a single logical document that provides a single coherent statement of meaning, establishes its own context and that has clinical attestation regarding who is making the statement.

Table 3. FHIR profiles

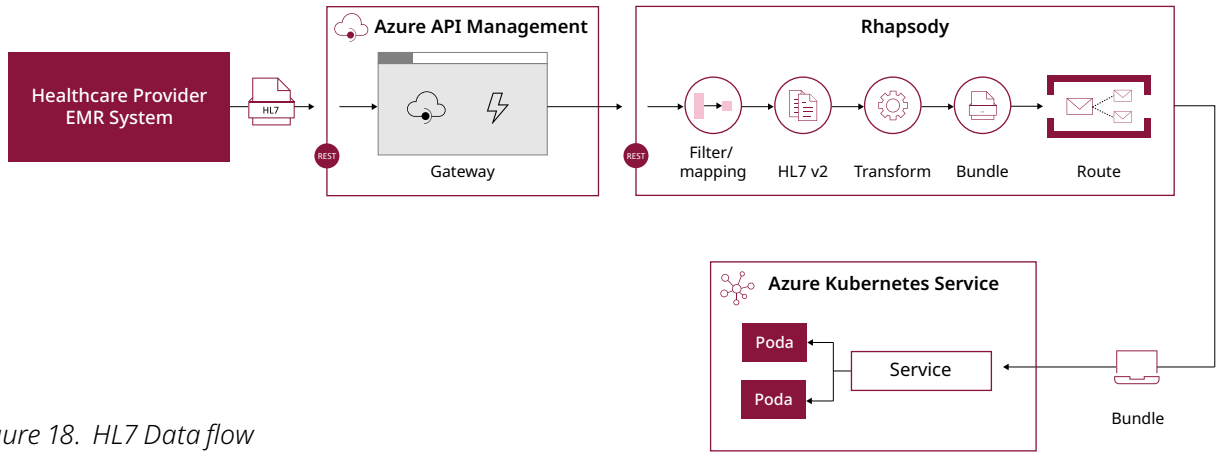


Figure 18. HL7 Data flow

6.2.3 Understand patient registration, creation and update processes to be implemented in your EMR

Integration with the QHIE-Hub requires healthcare providers to change certain existing workflows and processes within their EMRs. This section outlines patient registration workflows that need to be updated i.e., patient registration,, creation, and updates via the eMPI service. Detailed specifications for eMPI integration policies along with message structures are provided in FHIR specification documents shared as part of the onboarding resources

Based on the patient demographics data received from different healthcare providers, the Enterprise Master Patient Index (eMPI) service of the QHIE-Hub Platform creates a new Master Patient Record (MPR) or links patients to existing MPRs, using an internal, multi-step, matching algorithm. The eMPI also receives patient demographic data from the Ministry of Interior to ensure patient information is matched with the official demographics. Fields received from MoI include:

- **Names** – English and Arabic (up to 5 names in each)
- **Identifiers** – QID number, Visa / Passport number (with their statuses and expiry dates)

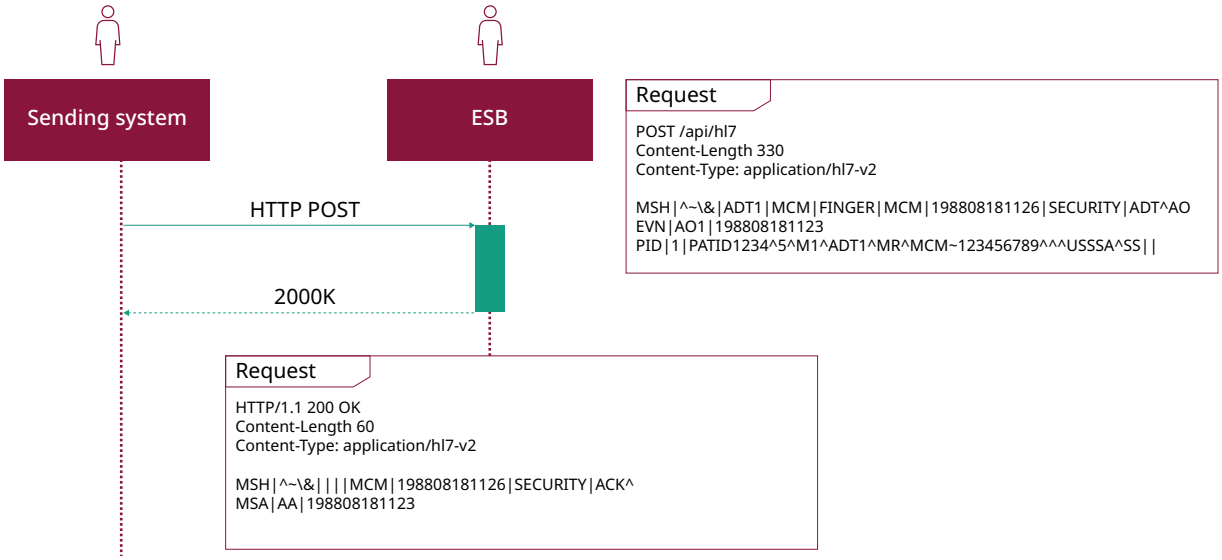


Figure 18.1. HL7 over HTTPs workflow

Event ID	Name	Definition
ADT_A01	Admit a patient	This event is sent upon a new patient encounter
ADT_A03	Discharge a patient	This event is sent upon patient discharge or to close patient encounter
ADT_A04	Register a patient	If the new encounter is for ambulatory care, this event should be sent
ADT_A05	Pre-admit a patient	When a new encounter is created with a pre-admit class, this event should be sent
ADT_A08	Update patient information	This event is used when updating a patient information with no other trigger event
ADT_A11	Cancel patient admit	This event is sent when moving the encounter type back from admit to pre-admit
ADT_A13	Cancel patient discharge	When the discharge event is to be cancelled and the encounter type is changed back to pre-admit or outpatient.
ADT_A25	Cancel Pending Discharge	The A25 event is sent when an A16 (pending discharge) event is cancelled, either because of erroneous entry of the A16 event or because of a decision not to discharge the patient after all.
ADT_A28	Add person information	The A28 event can be used to send everything that is known about a person to the eMPI server
ADT_A31	Update patient information	An A31 event can be used to update person information. The difference between A31 and A08 is that A08 is used to update patient information in a current episode.
ADT_A40	Merge patient information	This event is intended for merging or changing patient identifiers. It could be used to change patient identifiers on all the patient's existing accounts

Event ID	Name	Definition
PPR_PC1	Problem Add	The patient problem message is used to add problems from one application to another
PPR_PC2	Problem Update	The patient problem message is used to modify problems from one application to another
PPR_PC3	Problem Delete	The patient problem message is used to delete problems from one application to another
OML_O21	Laboratory order	This event can be used to send laboratory order messages
OMI_O23	Imaging order	This message is used in communication between the information systems involved in the fulfilment of the request directed to the imaging department, such as a Radiology Information System (RIS)
OMD_O03	Dietary order	A diet office needs to receive specific information, the most important being the diet order itself
OMG_O19	General clinical order	The function of this message is to initiate the transmission of information about a general clinical order that uses the OBR segment
ORU_R01	Results and observations Diagnostic report	The ORU message is for transmitting results to other systems
ORU_R01	Observation Result for Diagnostic Reports	Communicates results for diagnostics like imaging or pathology. (Same message structure as lab results, used differently contextually.)
OMP_O09	Pharmacy/treatment order	This event is intended for sending pharmacy requests
RAS_O17	Pharmacy/treatment administration	This event is sent for administration of medication
RDS_O13	Pharmacy/treatment dispense information	The RDS message may be created by the pharmacy/ treatment application for each instance of dispensing a drug or treatment to fill an existing order or orders
VXU_V04	Immunization	This event is sent for updating a patient record with immunization information
MDM_T01	Document Creation	This event is used to send a notification for original document creation with the accompanying content
MDM_T05	Document Addendum	This event is used to send a notification for addendum to a document without the accompanying content
MDM_T06	Document Addendum	This event is used to send a notification for addendum to a document with the accompanying content
MDM_T09	Document Replacement	This event is used to send a notification for replacement of a document without the accompanying content
MDM_T10	Document Replacement	This event is used to send a notification for replacement of original a document with the accompanying content with a Parent ID of the original document

Table 4. HL7 events

- **Contact details** – mobile and telephone numbers, email id, address in official format
- **Additional details** – Date of Birth, Gender, Nationality

As part of patient registration, creation, and update processes, the above details will be sent by MoPH to healthcare providers via the eMPI service. Healthcare providers are expected to store this information and update the patient records within their EMR. It is important to note that most of these fields are mandatory (except contact details) and they should not be changed by healthcare providers under any circumstances. Changes/corrections, if any, need to be done by individual patients directly with the Ministry of Interior via official channels.

The primary objective of the eMPI service is to reduce the operational overhead for healthcare providers in maintaining accurate and up-to-date patient demographics.

For each master patient record that is created, the eMPI service automatically generates an NHN (National Health Number) – a non-sequential, 10-digit unique identifier to be used as a backend number to exchange data with the QHIE-Hub. It must not to be used as a patient facing number. **Healthcare providers are required to configure their EMR systems to store the NHN number.**

To ensure compliance with the QHIE-Hub, healthcare providers need to modify business and technical workflows across the following processes:

1. New patient search and creation
2. Update existing patient records in eMPI
3. Update EMR with latest patient information from eMPI
4. Handle discrepancy with eMPI data

eMPI has up-to-date demographic information as it receives the data from Ministry of Interior and is updated based on the patient data received from different HCPs.

6.2.3.1 New patient search and creation using eMPI

At the time of new patient registration, healthcare providers must first search for the patient using the eMPI services of the QHIE-Hub. They must not register a patient directly and must take all necessary actions to avoid direct registration of patients without querying the MoPH eMPI service. Healthcare providers need to receive the patient's data from the QHIE-Hub and use the returned data (which will include additional demographic information) for registering new patients.

This search can be done with key identifiers via a "query request These key identifiers contain unique identifying information about patients such as QID number, Passport number, nationality etc.

Below is the list of acceptable search parameters for different types of searches:

1. Acceptable parameters for searching with key identifiers (outlined in the workflow below):
    a. QID + Birth date
    b. GCC ID + Nationality + Birth date
    c. Passport number + Nationality + Birth date
    d. Visa No. + Nationality + Birth date
    e. Medical Record Number (MRN) + Birth date – only for existing patients already registered through eMPI

Healthcare provider systems must be able to trigger a "retrieve request" to the eMPI system using the above combinations of parameters along with organization identifier. This request will fetch the detailed patient record for a maximum of one person as a response. Once patient data is received, healthcare providers must use this data for creating the patient record locally and subsequently when sending their clinical data to the QHIE-Hub. They must also send the locally generated medical record number.

Conditional referencing is used to validate the patient's data received by the QHIE-Hub. If no match is found, the process of linking or creating a new master patient record (MPR) will start in the QHIE-Hub. This is outlined in the workflow below.

Only when the above query/retrieve requests do not yield valid results, healthcare providers

may create a new patient and send demographic information to the QHIE-Hub.

There are three types of scenarios in which these Patient Records are created in the eMPI:

1. **First time visit (healthcare provider creates a new patient with identifiers in their local EMR based on patient identity policies issued by MoPH):**
    - This process is initiated when healthcare providers send a create request with identifiers such as QID, PPN, or Visa Number to the eMPI system (after a retrieve request from the previous stage has not yielded valid results).
    - An internal search for the patient is performed on the MOI database using the search parameters i.e., Identifiers, Nationality and Date of Birth (DoB).
    - Whether a matched person is found or not, a Master Patient Record (MPR) is created. The MRN of the patient from the healthcare provider is linked to the created MPR.
2. **Birth event for newborns:**
    - After a birth event, the healthcare provider needs to send the information to the QHIE-Hub by preparing a clinical bundle suitable for a newborn profile. A clinical bundle is a collection of data elements across a set of FHIR profiles into a single instance with a shared context. For a newborn, it must consist of:
        - Identifier (MRN number)
        - Patient Name (actual name or name linked to mother's name)
        - Birthdate
        - Gender
        - Link (details of the reference patient i.e., mother, including her name, identifier information, and other details within "Patient" resource)
        - Managing Organization (reference organization i.e., the hospital/clinic)
    - At this stage, newborn identities and names are not expected to be filled by the healthcare provider. However, the newborn's link to the mother/related patient is mandatory. Healthcare providers must ensure these details are sent.
    - The FHIR Server within QHIE-Hub Platform utilizes this bundle to create a new master patient record.
    - The eMPI system verifies a newborn by sending a retrieve request to the MoPH Birth Registry API with the MRN (Medical Record Number) of the baby from the hospital.
    - If the MRN is found in the birth registry system, the eMPI adds the birth registration number and other birth indicators to the MPR.
    - The eMPI also automatically establishes a link between the newborn and the mother, storing this link element in the MPR to define the mother-baby relation.
    - Once the name and QID are finalized and sent along with other details by MoI, the newborn MPR is updated
3. **Patients without any identifiers (unknown patient):**

Healthcare providers should establish internal policies and procedures for registering unknown patients. The designation "unknown patient" should only be used when the individual is truly unable to self-identify at the time of the encounter—such as in cases of unconsciousness, disorientation, or other forms of incapacitation—and not solely due to the absence of identification documents.

- Emergency departments may admit unknown patients for medical services or external referrals.
- A special profile for unknown patients is defined by MoPH, which does not require certain information like name, telecom, birthdate, nationality, and identifiers except their MRN (Medical Record Number) generated from the healthcare provider.
- Healthcare providers need to use this special profile to send clinical data to the FHIR server for unknown patients.
- When a create request is received for this type of patient, the eMPI does not create an MPR but just a patient record (orphan patient).

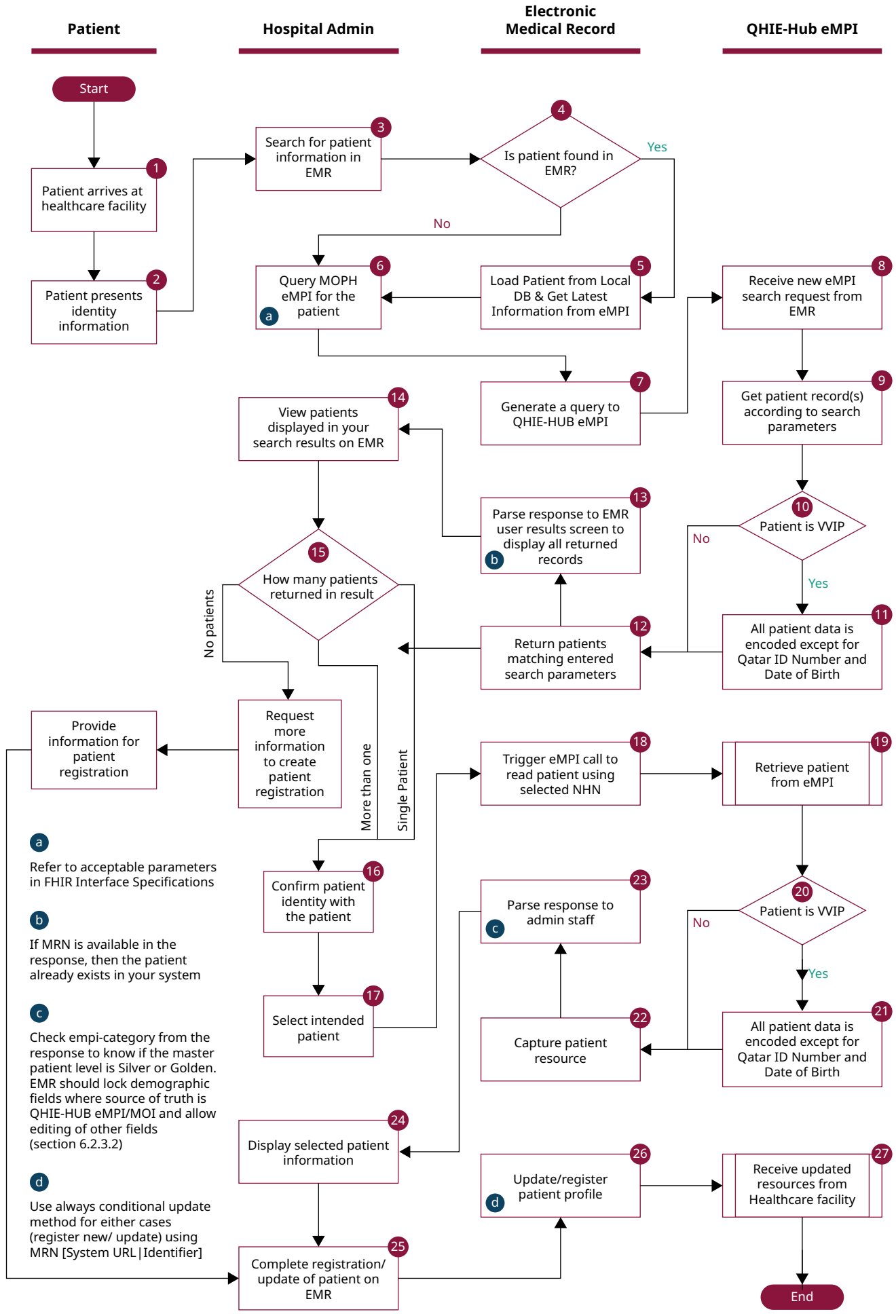


Figure 19. Patient Registration for Patients With Official Identifier (PatientWithIdentifier Profile)

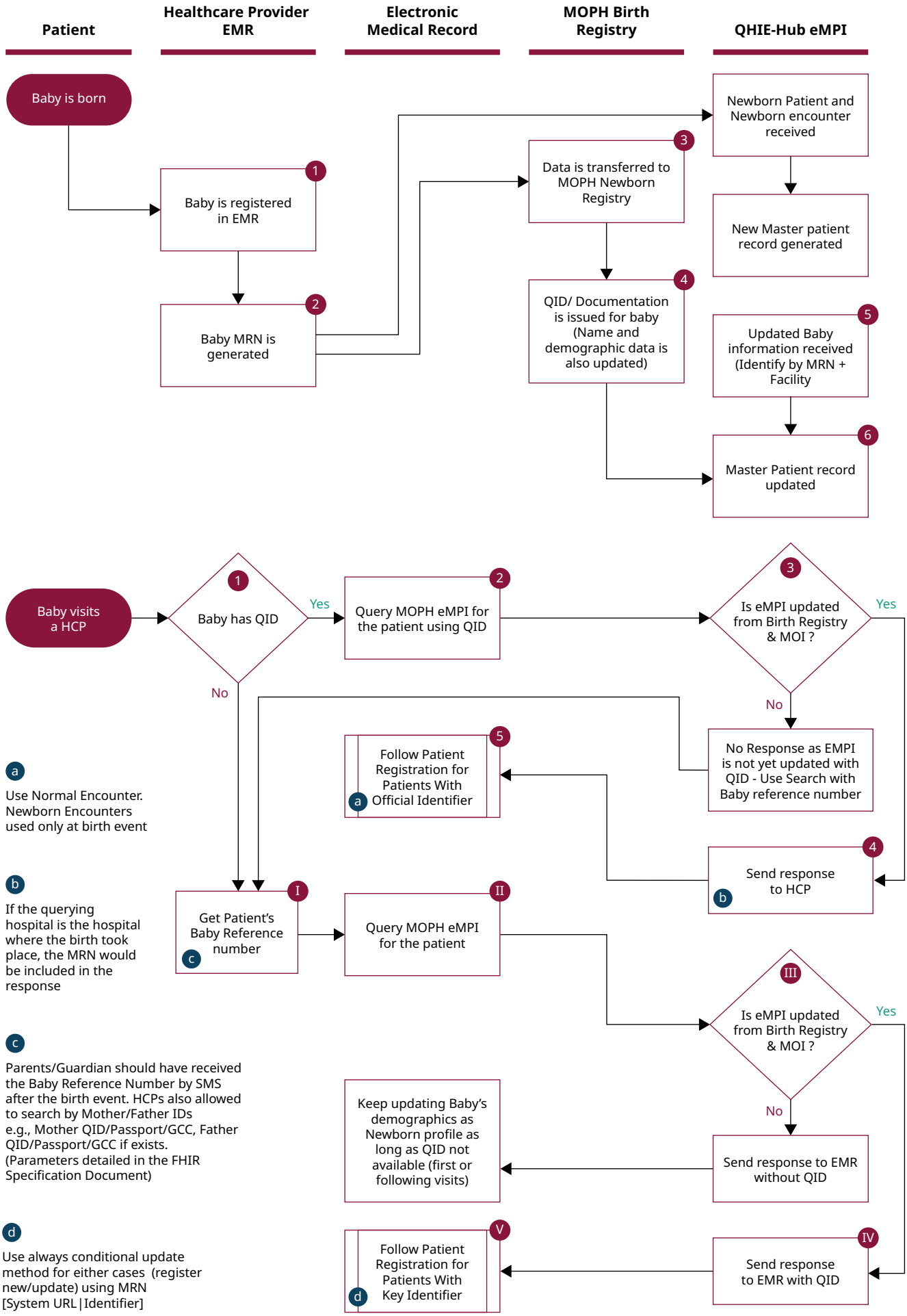


Figure 20. NewBorn Regsitration (NewbornPatient Profile)

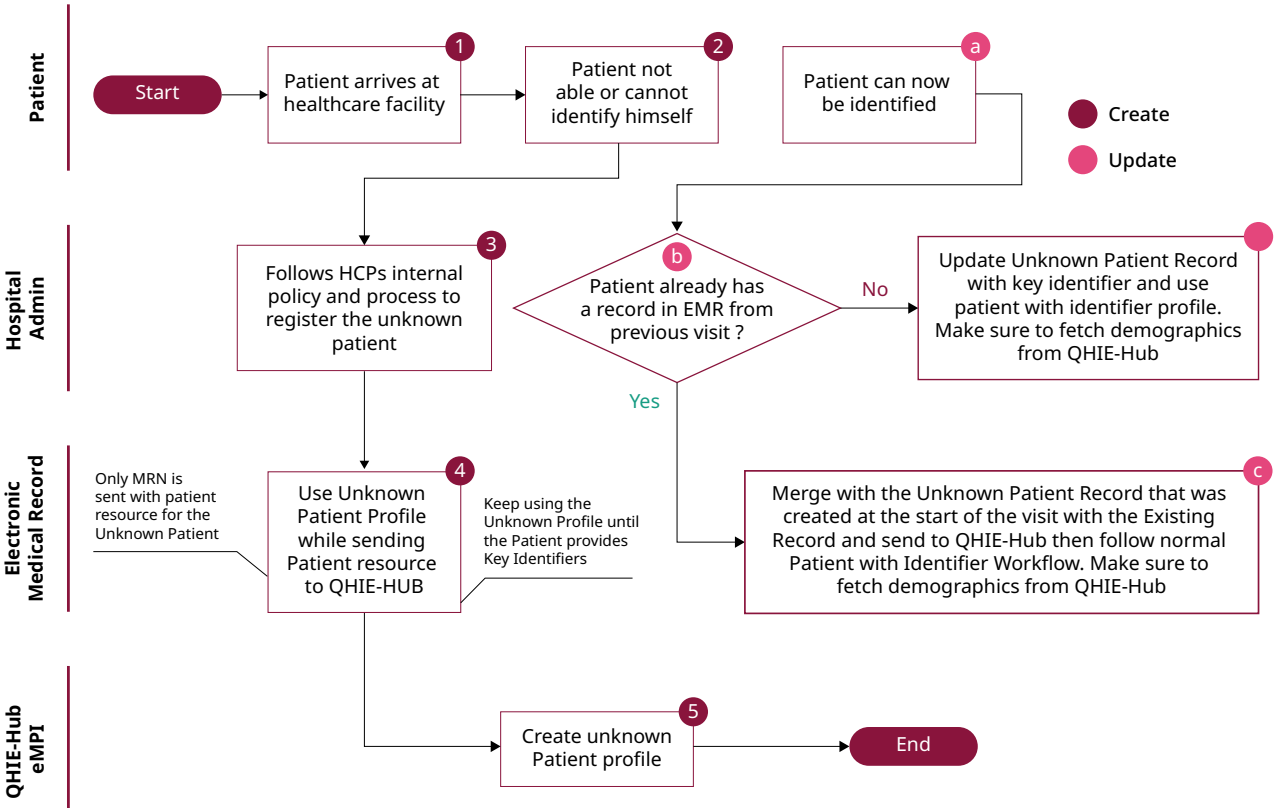


Figure 21. Process Flow for Unknown Patients

- Healthcare providers can use MRN to reference this patient, but querying with names and matching algorithms will exclude unknown patients.
- Once the healthcare provider identifies the patient, patient updates and clinical bundles should be sent with this identity. The eMPI automatically initiates the update process for these patients.

Whenever a patient is registered without their true identifier, i.e., newborn, unknown patient, the healthcare provider is liable for correcting this data on their systems as and when the true identifier of the patient is known.

6.2.3.2 Update existing patient records

Healthcare providers can search for existing patients through the same search methods (with and without identifiers). Additional parameters can be used for search with identifiers i.e., the patient MRN number and NHN number.

Once a master patient record (MPR) is created within eMPI, multiple healthcare providers may attempt to update it. However, to ensure the sanctity of the patient record within the QHIE-Hub, MoPH has determined the source of truth for various master patient elements as outlined below (subject to change by MoPH). Consequently, the eMPI system will automatically decide the correct data source to use based on the element and its corresponding primary source of truth before updating an element.

Health care providers MUST comply with the below table for locking down fields after querying eMPI.

1. **Update Telecom Data of MPR (allowed):**
   - When healthcare providers update the telecom data, it is checked and combined with the telecom data from MOI. The eMPI will store the latest number from the most recent HCP visit, the number from MOI, and the number entered by the Patient as part of their Personal Health Record solution registration.
   - The patient, using their Personal Health Record solution can select the number they wish to be used as their primary number. This number will be used to be displayed across all MoPH national solutions.
   - If a patient does not enter their preference, then the number used to register in their

Personal Health Record solution will be used by default. If this is not available, the latest number from the last visit to a healthcare provider will be displayed.

2. **Update Newborn MPR:**
    - A newborn MPR is created without identifiers and names by sending a clinical bundle.
    - Once the newborn's name is decided, the healthcare provider/guardian needs to update the birth registration system
    - After the ID of the newborn is assigned by MOI (Baby Reference Number), the birth registry portal is updated by MoPH
    - eMPI sends a query request to the birth registry to get an updated birth record list, which is used to prepare update MPR requests.
3. **Update Deceased MPR:**

For For deceased patients, healthcare providers may send deceased data elements. They can also locally update the patient data. However, the MPR is not updated in the case of deceased individuals since the eMPI uses MOI data as the source of truth.

6.2.3.3 Update healthcare provider EMR with latest patient information

An update to the master patient record (MPR) in eMPI can occur due to changes in MOI data or due to changes made by another healthcare provider. Consequently, by best practice, healthcare providers with a patient linked to that MPR should always update their records. This is not mandatory, but highly recommended.

The healthcare provider is typically made aware of the change during a patient encounter. At this time, they must update their existing patient records based on the data received from eMPI (via the eMPI retrieve request).

6.2.3.4 Handle discrepancy with eMPI data

In case a patient reports or a healthcare provider notices discrepancies with the eMPI data, particularly where the Ministry of Interior is the source of truth, the healthcare providers may, under exceptional circumstances, update their local patient record (e.g., correcting an incorrect name before an urgent treatment pending an international insurer's approval). However, doing so may result in eMPI automatically executing actions associated with **Update Identifiers or demographic information of MPRs.**

Hence, healthcare providers are advised to let the data remain as-is and guide patients to get these discrepancies resolved/information updated directly with the Ministry of Interior after the normal verification process.

MoPH may contact healthcare providers to collect a consolidated list of discrepancies for a bulk update in the MoI database. However, the viability of this approach is being ascertained, until which time this process cannot be followed.

	Record lock status			
Patient Demographic	**Gold**	**Silver**	**Special Field**	**Definition for the Special Field**
QID	Y	N	Expiry Date/ identifier. period	**patient.identifier.period:** Indicates the validity, start date and expiry date of an identifier. If the validity information is available from MOI, it will be passed in the
PPN	Y	N		
Visa ID	Y	N		
GGC ID	Y	N		
MRN	Y	N		
Baby ID	Y	N		
Given Name	Y	N	Name Language name.given name.family	**name.extension.NameLanguage.coding:** will represent the language used to express the given and family name of the patient within the same array index. This follows a defined valueset and can contain an example of 'en' The last name of the patient is used within name. family while first name and middle name1, middle name2, middle name3 is used within the array name. given.
Family Name	Y	N		The patient record returned from eMPI as golden should have its fields locked according to the golden record lock status; however, if the patient record is returned with only arabic name, then the english name can be modified/added by the healthcare provider. Healthcare providers should not combine middle names and send
Gender	N	N		
BirthDate	Y	N		
Marital Status	N	N		
Nationality	Y	N		
eMail	N	N		
Person Type	Y	N		
Active	Y	N		
Multiple Birth	N	N		
Contact Information	N	N		
General Practitioner	N	N		
Deceased	N	N		
Communi-cation (language)	N	N		

Table 5. Source of Truth for information on the elements of the master patient record (continued...)

	Record lock status			
Patient Demographic	Gold	Silver	Special Field	Definition for the Special Field
Phone Number	N	N	ID + System + Value + Use + Rank	**telecom.id:** Represents the source of the telecom for the patient. **"HCP"** indicates the telecom entry was provided by a Healthcare Provider. **"PHR"** indicates the telecom entry was provided by the patient through their PHR application. **"MOI"** indicates that the telecom entry was provided by Ministry of Interior for the patient. **telecom.system:** indicated the system for the telecom entry. The allowed list and definitions exist within the defined valuset. **telecom.use:** indicates the use for the telecom entry. The allowed list and definitions exist within the defined valueset. **telecom.rank:** indicates the order in which this telecom entry was combined to the master patient record, where the first entry gets rank '1', second entry gets rank '2' etc. **telecom.value:** indicates the actual value of the entry e.g. Phone Number HCPs are recommended to use PHR and/or HCP with highest rank as the most updated record availed by the Patient, MOI where others are not available. HCP numbers will always fall under HCP category.
Address Information	N	N	Unit + Building Number + Street Number + Zone Number	**Inwani address:** Inwani address which represents the official "blue box" address can be represented according to the below mapping while sending and receiving data from QHIE-HUB **BuildingNumber:** address.extension.url = https://fhir.moph.gov.qa/StructureDefinition/AddressBuildingNumber, the valueString element is mapped to Building Number **UnitNumber:** address.extension.url = "https://fhir.moph.gov.qa/StructureDefinition/AddressUnit", the valueString element is mapped to Unit Number **ZoneNumber:** address.extension.url = "https://fhir.moph.gov.qa/StructureDefinition/AddressZone", the valueString element is mapped to Zone Number **StreetNumber:** address.extension.url = "https://fhir.moph.gov.qa/StructureDefinition/AddressStreetNumber", the valueString element is mapped to Street Number

Table 5. Source of Truth for information on the elements of the master patient record


Mandate, policies &guidelines
Overview of national solutions
A. Get familiar with QHIE Hub
B. Get ready to onboard
Onboarding Roadmap
Implementation Plan
Change management
Meet requirements (security, integration, data)
You are here
Connect to sandbox to develop APIs
Map & transform data
Clean historical data
Validate patient demographics
Connect to Pre-prod to test workflows
Training
Complete onboarding assessment
Actual onboarding/production
Go live
GO LIVE
C. After you onboard
Drive adoption
Monitor data quality

6.2.4 Develop Interface Messaging Scripts

To share the data with the QHIE-Hub using either FHIR or HL7 standards, healthcare providers are required to develop scripts.

HCPs are required to connect to the Sandbox environment to develop APIs. They can leverage the Developer Portal published by MoPH as they build their APIs for testing their scripts.

This section outlines the key steps in the process.

1. Review the detailed Interface Specification documents published by MoPH that explain how APIs for FHIR Clinical, eMPI and Terminology Services can be created
2. Connect to the MoPH sandbox environment to test the APIs using synthetic data

Healthcare providers must utilize the sandbox environment to test below APIs:

- FHIR R4B clinical APIs
- HL7 V2.5.1 pipelines
- Terminology Mapping APIs
- eMPI service API
- API Playground for healthcare providers to test their scripts using the "Try It" option

6.2.4.1 Connect to Sandbox to develop APIs

While healthcare providers continue to develop the APIs, they may establish a connection with the sandbox environment to test these APIs. Detailed guidance on how to connect with the Sandbox environment has been shared in Chapter 6.1 Security & connectivity.

6.3 Data

This section covers key requirements and processes that all healthcare providers need to follow within the data domain so that they enable exchange healthcare data after their onboarding. It also intends to provide guiding principles on how data will be defined, managed, classified, standardized, and shared between the QHIE-Hub and its stakeholders within the healthcare ecosystem. There are 4 steps as summarized in the Figure 22.

6.3.1 Implement data coding & terminology standards

Healthcare coding and terminology standards are the foundation for achieving semantic interoperability for sharing health information among provider systems and integrating health data with national solutions to provide better care to the public of Qatar. Healthcare providers in Qatar use various data standards for different data domains such as diagnosis, laboratory, immunization, etc., which is one of the biggest barriers to meaningful data exchange. Therefore, before connecting with the QHIE-Hub, all healthcare providers must prepare their systems to adhere to the national terminology and coding standards.

The QHIE-Hub program website has a login-based section to download all code systems stated in the National Terminology Directive (including licensed code systems such as ICD10-CM, SNOMED-CT, LOINC, CPT, CDT) that healthcare providers must download and apply to their systems. The preferred method is to directly apply these code systems without the need to host any local-to-national cross-maps on the QHIE-Hub Terminology management portal. However, in the interim, healthcare providers can create and host local-to-national cross-maps on the QHIE-Hub Terminology management portal to support translation (wherever applicable) and to adhere to national coding standards during data exchange with the QHIE-Hub.

Figure 22. Steps to transform data

6.3.1.1 Access the QHIE-Hub Terminology management portal

This section explains how healthcare providers can use the Terminology Management System to access terminology resources as well as to create and host concept maps. The Terminology Management System plays a crucial role within the QHIE-Hub, aiding healthcare providers and national authorities in effectively managing and structuring clinical and local terminology resources. By centralizing codes and terminology in a repository, this service facilitates their seamless integration across various systems and applications within the national healthcare landscape. This tool ensures the uniformity and precision of data employed by healthcare organizations, thereby contributing to enhanced consistency and accuracy across the board.

At the time of onboarding, the data liaison nominated by a healthcare provider will be provided credentials to log in and will be assigned the role of a Terminology Author in the Terminology Management System.

This person will be able to access the Terminology Management System and view and download the national code systems. The Terminology Author can also create and send the local Code Systems, Value Sets, and Concept Maps for approvals.

The QHIE-Hub program team will publish a detailed end-user manual for healthcare providers to understand the functionality of the system and how they can access it as Terminology Authors.The key modules of this system include:

1. Code systems
2. Value Sets
3. Concept Maps
4. Approval Requests

This section provides additional details on key modules of the system.

1. **Code systems**

   This module defines which code systems currently exist in the QHIE-Hub and how they can be utilized. Through this module, the Terminology Author can:

   - View Code Systems
   - Filter the Code Systems
   - Create local Code Systems
   - Edit local Code Systems
   - Send the local Code System for Admin Approval
   - Clone the local Code System
   - Send to Retire the local Code System
   - Delete the local Code System

   To ensure a newly created code system can be utilized, it must have a unique concept code attached to it. Concepts can be added right after the user saves the code system, or in the code system page afterwards. Code Systems without a concept code will not be sent for Admin Approval.

   Through this module, the Terminology Author can:

   - View Concepts
   - Filter Concepts
   - Add Concept
   - Import Concepts
   - Add and Edit Concepts Property
   - Delete Concept

2. **Value set**

   A Value Set resource instance specifies a set of codes drawn by one or more code systems, intended for use in a particular context. Value sets link between Code System definitions and their use in coded elements.

   Through this module, the Terminology Author can:

   - View Value Set
   - Create Value Set
   - Include and Exclude Codes
   - Include & Exclude Filter
   - Expand Operations
   - Edit Value Sets
   - Filter Value Sets
   - Delete Value Sets
   - Send Value Sets for Admin Approval
   - Clone Value Sets
   - Send Value Sets for Retirement

Healthcare providers are not expected to create any value sets for the QHIE-Hub national solutions. They must use the approved value sets available in the terminology mapping portal. Therefore, the privilege to create or update will not be enabled for healthcare providers. This authorization will only be granted on an exception basis for specific use-cases as and when required.

3. Concept Maps

A concept map provides a mapping from a set of concepts defined in a code system to one or more concepts defined in other code systems. These concept maps are uploaded/downloaded in CSV formats. A pre-defined template with the necessary fields (such as source code system, target code system, source code, source display, target code, target display, equivalence) can be downloaded directly from the terminology management portal. Users must upload their Concept Maps in the provided template format. Through this module, the Terminology Author can:

- Create Concept Maps
- Edit Concept Maps
- Filter Concept Maps
- Send the Concept Map for Admin Approval
- Clone the Concept Map
- Retire the Concept Map
- Add maps from source code system to target code system
- Edit maps from source code system to target code system

4. Approval requests

Every local code system, value set, and concept map must be submitted to the MoPH Terminology Admin through the Terminology management portal to be enabled in the Prod environment. Once the user has completed the authoring of the local code system and concept maps, they need to raise an approval request. The user can view and track their requests status in this module.

The detailed steps to access the portal are mentioned below:

- The healthcare provider nominates a data liaison to access the terminology portal once contacted by the facility manager from MoPH. Once nominated, MoPH will register an account for the user in the User Management Module. The user is sent an automated email with credentials to their registered e-mail address.
- As a first step, the user needs to install the Microsoft Authenticator app on their mobile device to validate when they are challenged by a multi-factor authentication. Instructions to download Microsoft Authenticator can be followed here: https://www.microsoft.com/en-us/security/mobile-authenticator-app
- Once done, the user needs to visit the URL: https://terminology-management-ppr.MoPH.gov.qa/. They need to enter their e-mail address/QID number and password and click the **Sign-in** button.

1 The user must define the method of authentication to log-in to the Terminology Management Service for the first time. They must select their country/region code, provide the mobile phone number and choose a preference to authenticate

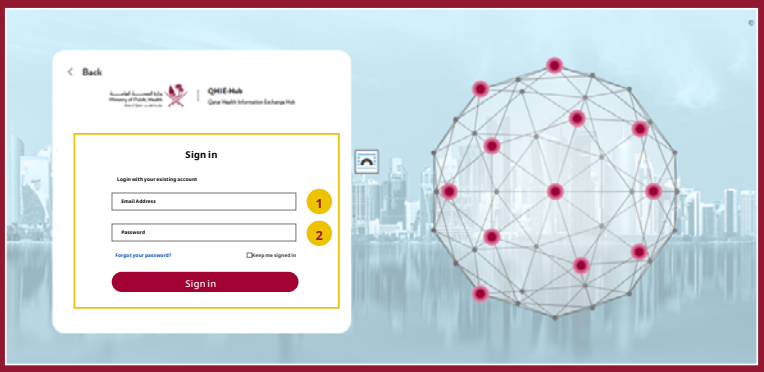


Figure 23. Landing page of Terminology management portal

2 At this stage, the user is challenged by MFA and will receive an SMS text message with a six-digit verification code that needs to be entered. After the first login, the user needs to define a new password.

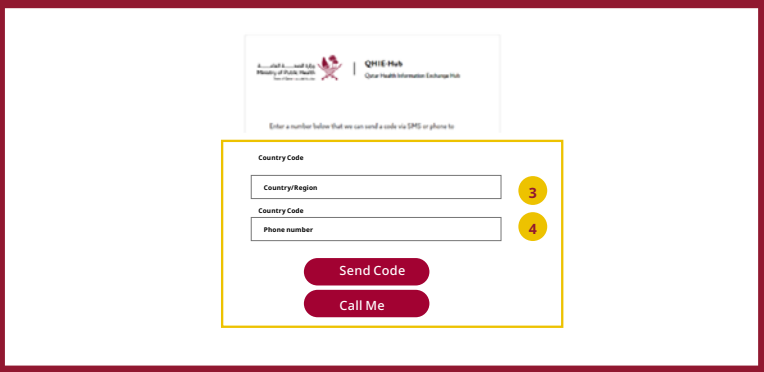


Figure 24. MFA Login screen

3 Once logged in, the user is required to agree to the terms of service, and check "I agree" box

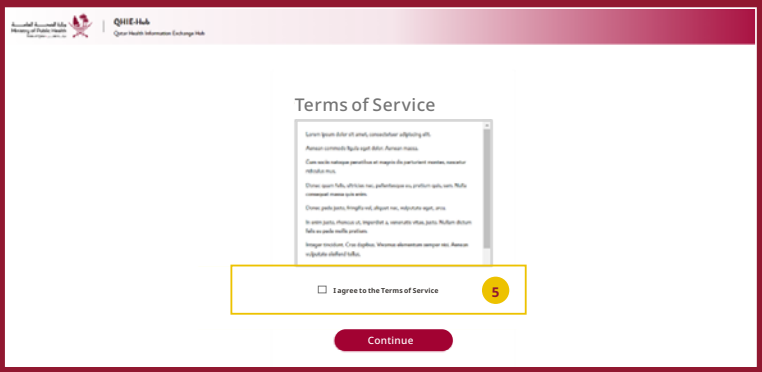


Figure 25. Terms and conditions

6.3.2 Choose Data Exchange Standards

Healthcare providers are required to use Fast Healthcare Interoperability Resources (FHIR R4B) APIs to share their data with QHIE-Hub. However, MoPH will also facilitate use of Health Level Seven (HL7 v2.5.1) as an alternate approach till December 2025 healthcare providers upgrade to FHIR R4B standards. All healthcare providers must adopt either of these standards for exchanging healthcare data with the QHIE-Hub.

All healthcare must use FHIR or HL7 APIs to share real-time data with the QHIE-Hub. HL7 is provided as an interim approach until December 2025.

As part of the onboarding process, historical electronic health records and the patient demographic data need to be sent via these APIs. More details on the overall data migration process and how to access related services (like eMPI, FHIR, and Rhapsody) during onboarding are available in Chapter 8.2 Execute historical data migration. Healthcare providers who are unable to use FHIR/HL7 APIs to migrate historical data may request approval for bulk-upload of CSV files as a last-resort option with justification before onboarding.

6.3.3 Build Pipelines as per Target Datasets

In FHIR, healthcare data is broken down into categories such as patients, laboratory results, and insurance claims, among many others. Each of these categories is represented by a FHIR Resource, which defines the component data elements, constraints on data, and data relationships that together make up an exchangeable patient record.

Each Resource contains data elements necessary for specific use cases and links to relevant information in other Resources. For example, the Patient Resource contains basic patient demographics, contact information, and links to a clinician or organization stored in different resources.

A collection of these resources and elements profiled to serve specific use cases constitutes the target dataset. Based on functional requirements and clinical inputs, the QHIE-Hub has defined its own target dataset that contains all profiles to be used across its solutions. Elements within each profile have defined data types, and some have value sets or code systems that constrain the values that can be used.

The QHIE-Hub has categorized all the elements into five types:

1. **Mandatory**
   - This element is mandatory, and the system message will only be accepted by the QHIE-Hub if the element is present.
   - Sending this information is essential and must be complied with, to ensure the message's acceptance by the QHIE-Hub.
2. **Conditional**
   - This element's data sharing requirement is conditional based on a condition set in the "Description" column.
3. **Optional - Must Support**
   - The QHIE-Hub will accept messages that do not include this field, and as such it is considered optional.
   - However, if your system already captures this information, you must include it in your system message to the QHIE-Hub. This is because MoPH has deemed this field to contain vital clinical information and must receive it from healthcare providers.
   - This requires your compliance as MoPH may audit this in the future.
4. **Optional – mandatory within 2 years:**
   - The QHIE-Hub will accept messages that do not include this field, and as such it is considered optional.
   - However, this field will become mandatory within 2 years, as the description states, thus requiring healthcare providers to plan on including this field in their future messages
5. **Optional:**
   - This element is optional.
   - It is acceptable if the system message does not contain this field.

All healthcare providers must capture and transform the above data from their source systems as per the specifications outlined in the target data set of the QHIE-Hub. This is imperative to enable a real-time data exchange with the QHIE-Hub.

Healthcare providers are also required to organize their historical data as per the target data sets so that it can be migrated to the QHIE-Hub during their onboarding. **Healthcare providers will only be deemed to be ready for onboarding only when they conform with the target datasets that includes all the mandatory fields for all the resources.**

Once the target dataset is finalized, healthcare providers must configure the interfaces and develop pipelines to connect to the QHIE-Hub based on the selected messaging protocols (FHIR 4B/HL7 V2.5.1).

6.3.4 Execute Data Quality Profiling and Quality Assessment

Data profiling is the practice of efficiently verifying and documenting the characteristics of data by analyzing a given data set and its metadata. It is used to understand the interconnections between the data across various production platforms while performing data assessment, data mapping, data cleansing, and reconciliation. **All healthcare providers must execute data profiling techniques and improve the quality of their datasets before sharing data with the QHIE-Hub.**

There are 7 data quality criteria that healthcare providers are expected to meet through profiling:

1. **Completeness:** The percentage of stored data with respect to the potential 100% of a particulate record. It is a measure that describes the frequency of data attributes being present v/s absent in a data set (e.g., % of encounters that have Encounter ID attribute filled)
2. **Uniqueness:** The extent to which no instance of data is registered more than once meaning that the data contains only one record for each entity it represents, and each value is stored once (e.g., there is only one master patient record for a patient with a given QID)
3. **Timeliness:** The level to which the data represent the latest clinical observations at the requested time (e.g., time difference between a patient being discharged and a discharge summary message sent to the QHIE-Hub)
4. **Validity:** The degree to which data corresponds to acceptable syntax (e.g., format, type, range) and standard definitions (e.g., ICD-10-CM, LOINC)
5. **Accuracy:** The degree to which data matches the agreed source of truth (e.g., prescription history in the QHIE-Hub matches the original data in the source facility)
6. **Consistency:** The absence of difference when comparing two or more representations/recordings of a data element

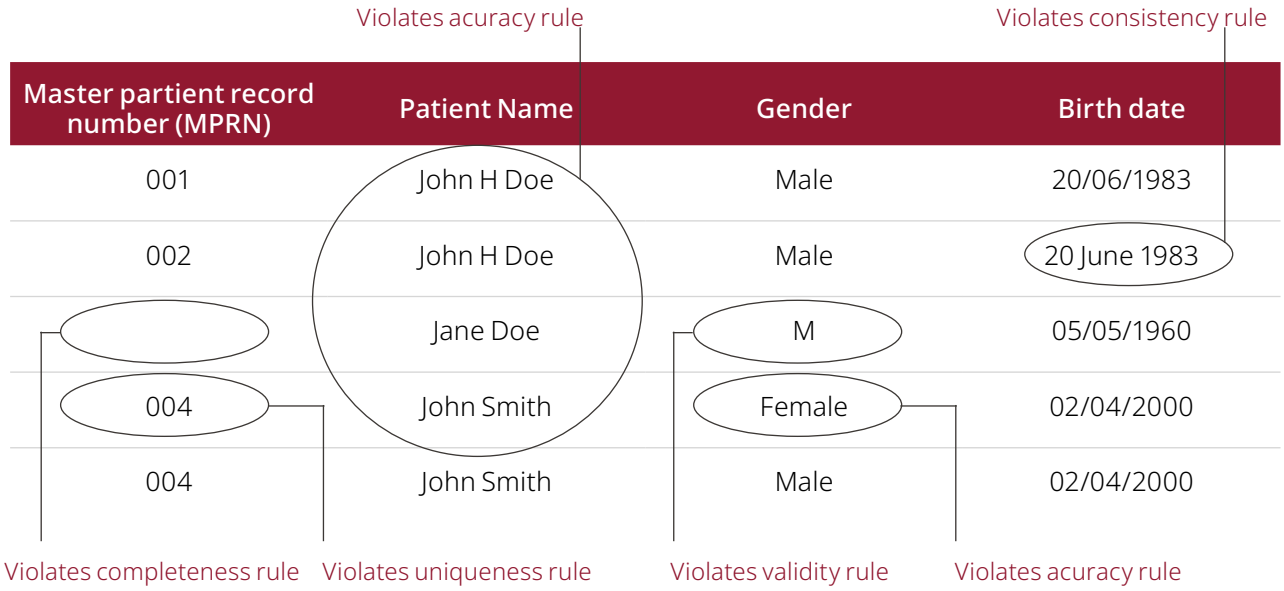


Figure 26. Example of incorrect data records

against a definition, across systems or through processes

7. **Plausibility:** The degree to which data is "believable." Extreme values and/or values that contradict real-world expectations are key concerns for the plausibility criterion and may uncover issues in data capture or transformation, that are not captured under the other criteria mentioned above (e.g., a prostate cancer diagnosis on a female patient or a prescription requested for a deceased person)

A detailed list of business rules is available in the Data migration guide provided with the onboarding handbook. Healthcare providers are required to implement these in their source systems to ensure data shared with the QHIE-Hub is not rejected.

Healthcare providers can also leverage the Azure Explorer tool to upload and assess their historical data in CSV format and to receive detailed error-reports for data quality improvement. A detailed guide on how to leverage this tool is provided in Chapter 8.2.3 Meet pre-requisites of the migration method & load data in prescribed sequence.

6.3.5 Validate patient demographics

One of the first resources that healthcare providers need to validate is the patient resource that contains all patient demographic data. Accuracy and integrity of this data is critical to ensure that a healthcare provider can use the QHIE-Hub platform's eMPI service for all patient registration / creation immediately after onboarding – a process that is mandatory

Table 6. Patient demographics template

#	CSV Field	Format	Example
01	QID	11-digit number	28425001234
02	DOB	Date of birth using the following format <DD-MM-YYYY>	19-01-1991
03	Passport No.	Passport unique identifier for the patient which can be of a string type	00126524
04	Nationality	MOI code standards **(refer to: Nationality value set)**	634
05	First name	String	
06	Middle name 1	String	
07	Middle name 2	String	
08	Middle name 3	String	
09	Last name	String	
10	Gender	<male | female | other | unknown>	Female
11	Phone	String	
12	Visa	String	
13	MRN	Medical record number used by the healthcare facility	
14	Mother QID	11-digit number	27411874124
15	Patient registration date	Registration date using the following format <DD-MM-YYYY>	20-02-2024

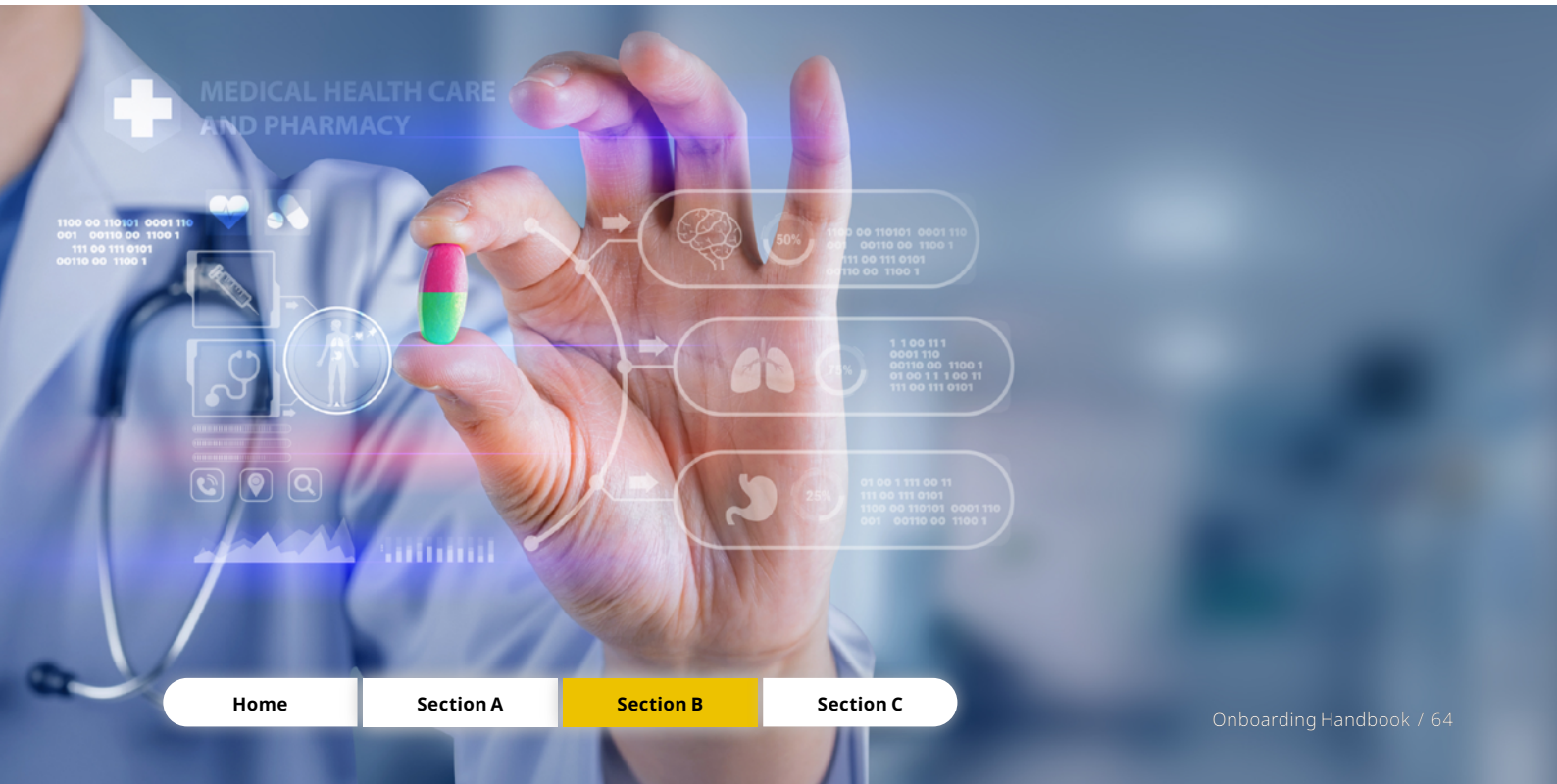
for all healthcare providers to adopt during onboarding.

Integrating with the eMPI service and successfully migrating patient demographics is an important milestone in the overall onboarding journey. To move forward, the healthcare provider should achieve full matching of their patient demographic details with the eMPI database which is updated with the demographic data from the Ministry of Interior.

A healthcare provider can use the eMPI tool to validate their full patient database before migrating the actual data to the Prod environment during Go-live stage. Below are the steps to use the tool:

- Extract all patient demographic data from the EMR and create a CSV file the eMPI guide, target data set and the data migration guide.
- Install and configure the Microsoft Azure Storage Explorer client based on steps outlined in Chapter 8.2.3 Meet pre-requisites of the migration method & load data in prescribed sequence. This is also the tool that will be used to eventually migrate all data to the Prod environment (in case a healthcare provider chooses the CSV data migration option).
- Apply the naming convention rules to name the file and upload it using the Microsoft Azure into the Input folder.
- Notify the assigned facility manager when the patient demographic CSV data file is successfully uploaded. The Facility manager will trigger the eMPI tool to run the patient matching algorithm on the file and generate a data quality report **within 48 hours.**
- Once completed, the output file will be available in the Output folder.
- Analyze the output file and fix all the errors within the source systems to ensure that patient records are complete and accurate.

In this manner, the healthcare providers must clean their entire patient demographic data before loading it into the QHIE-Hub platform in the Prod environment. They must discuss the number of runs / batches needed with their facility manager. The final match report must be saved and submitted as part of the onboarding review process.



CHAPTER 6.4

ePrescription and Digital Pharmacy (eMeds):

This section is intended to guide healthcare providers and pharmacies as they get onboarded to the ePrescription and Pharmacy Network solution. It provides an overview of the features of the solution, different methods to access it and outlines requirements that are specific to the method of access chosen by the healthcare provider.

6.4.1 Overview of the solution

The ePrescription and Digital Pharmacy is a system that allows prescriptions to be issued, dispensed, and tracked electronically across all healthcare providers and pharmacies. The main objectives of this solution include digitization of all prescriptions, providing a faster prescribing and dispensing process as well as safeguarding prescribing and dispensing practices. The prescriptions considered by the solution are primarily discharge and outpatient prescriptions (i.e., the medicines are taken home by the patient) which can be dispensed from any pharmacy.

Adoption of the Qatar National Drug Code system (QNDC) for drug code / classification and ICD10-CM and SNOMED CT for diagnosis are pre-requisites to use the solution. Furthermore, adoption of the GTIN/Serial number is also mandatory as a healthcare provider or pharmacy begins their onboarding to the e-Prescription and Digital Pharmacy (eMeds) solution and the Qatar Pharmacy Track and Trace System (QPTTS).

The patient search function of the solution utilizes the eMPI service of the QHIE-Hub platform. However, accessing the solution in a standalone manner does not require eMPI integration (covered later in this section).

As outlined in Section A and shown here, the solution has three modules. Below are the salient features of these modules (described for standalone access via the website which has the most comprehensive functionality):

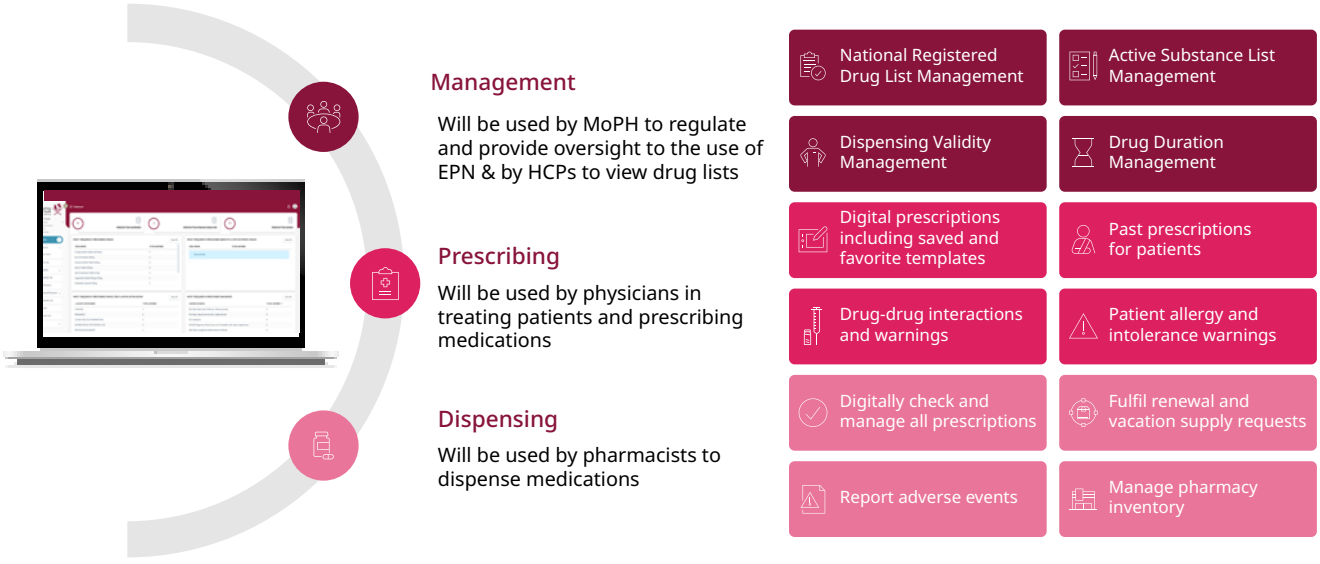


Figure 27. Overview of eMeds modules and features

1. **Management Module**

   a. This module can be accessed by both physicians and pharmacists. It consists of the "National Registered Drug List" which is synced with the Qatar National Drug Code system (QNDC) database and is used to provide drug and active substance information.

   b. Users can view the drugs' name, type (brand or generic), category (narcotic, psychotropic, uncontrolled, or controlled), restriction (OTC or prescription), creation date and modified dates. Users can also view the defined drug prescribing rules based on prescription types (which includes information like maximum frequency, maximum dosage quantity, maximum refill number, maximum order quantity, maximum duration) and the prescriber specialty information (i.e., allowed prescribers who can write the drug). It also provides the Drug Formulary Information by redirecting users to the Qatar National Formulary (QNF) website.

   c. This module also consists of the "Active Substance List" where users can see the active substance name and their categories such as Narcotic / Psychotropic or Controlled / Uncontrolled.

2. **Prescribing Module**

   a. This module can only be accessed by physicians who are a part of clinics/ hospitals etc. It consists of "Writing prescriptions component" where prescribers can search for a patient (using identifiers such as QID, Passport Number or NHN number), view their allergy & intolerance information, view medication reconciliation, save the prescription as a draft, preview the prescription, view drug interactions / warnings, and sign or co-sign the prescription. It also shows prescribers their top drugs, diagnoses and prescriptions to complete the prescription faster (a list that can be modified by users as needed).

   b. When prescribing, users must add at least one diagnosis to add drugs in the prescription. They can search diagnoses by their ICD10-CM codes or their names. All levels of ICD10-CM diagnoses codes can be searched and added.

   c. For each drug added to the prescription, the prescriber must enter instructions such as dose quantity, frequency, route, duration, and refill.

   d. When the prescriber saves the prescription as a draft prescription, the system checks prescribing rules defined by MoPH. These include maximum dosage quantity, frequency, refill etc. along with the prescriber's specialty to verify if they are allowed to write the drug. In case of narcotic or psychotropic drugs, a prescriber's license to write such drugs is also verified.

   e. When the prescriber proceeds to sign the prescription, the system displays drug warnings and interactions. It also enforces any co-sign requirements based on the type of practitioner using the platform. Once signed, the system generates and shows the prescription number on the screen and sends an SMS to the patient with their prescription status.

   f. The prescriber can edit a signed or pending for signature prescription until it is not dispensed, partially dispensed, or cancelled.

   g. This module also consists of "Renewal Requests component" where physicians can approve or reject renewal of prescriptions requested by pharmacists. Renewal requests are triggered to the same prescribing physician and cannot be requested from different physicians. If approved, the system redirects physicians to the prescription signature page to check the interactions before they sign the prescription. The system then sends a notification to the patient and the pharmacist about approval and rejection. The patient also gets a notification on their Personal Health Record Application.

3. **Pharmacy Module**

   a. The pharmacy module allows pharmacists to dispense prescription drugs, request and approve vacation supply, request renewal prescriptions, digitize prescriptions and record all processes. Prescription drugs are verified from the Qatar Pharmacy Track and Trace System (QPTTS) that has a real-time exchange of information with the ePrescription

and Pharmacy Network solution across drugs dispensing, return, cancellation & destruction processes.

b. To dispense drugs against a signed prescription, a pharmacist needs to search for a patient using their QID, Passport Number, MRN, NHN and Prescription code.

c. The pharmacist then needs to enter the information such as the Barcode and Serial Number of the drug to be dispensed into the relevant fields. If the prescription drug is not available, the "Equivalent" button can be used to find equivalent drug information for dispensing.

d. The system also provides warnings such as pregnancies, drug interactions, substance warnings, side effects etc. to the pharmacist at the time of dispensing. It checks for drug information, maximum dose and other defined rules during the dispensing phase to prevent dispensing entries that violate these rules.

e. Before dispensing, the pharmacist must verify the drug GTIN barcode number and serial numbers from QPTTS. The system will not perform the dispense button operation without verification.

f. The pharmacy module also has a process to return or destroy a dispensed drug. Return is only allowed 24 hours after dispensing, after which the drug is not returned but is directly destroyed. The drug return or destruction information is transmitted to the QPTTS service during this process.

g. This module also has the "Prescription renewal request" which is a process to request renewal of a completed prescription by the pharmacist on behalf of the patient. Renewal request is only allowed when the usage end date of all drugs of the prescription has expired. This request is sent to the prescribing physician for approval or rejection.

h. The Pharmacy module allows digitization of paper-based prescriptions by allowing pharmacists to write them in the system and save them as electronic prescriptions.

6.4.2 Consent settings

Patient consent will be required to grant a pharmacist who is dispensing medications the permission to view all medications that either have been prescribed to a patient and/or are currently being used by the patient.

The default setting is for sharing this data with all pharmacists for all patients. However, patients have the option to change these share settings at any time through their Personal Health Record profile.

By de-selecting this option selected, the pharmacist will only be able to view medications that have been dispensed from that specific pharmacy to a patient.

6.4.3 Access methods

Access and integration to the ePrescription and Pharmacy Network (eMeds) solution is achievable through two methods. The choice of method depends on the nature of the entity, preference, and technical capabilities.

The two methods include:

1. Standalone access (either via the website or embedding the URL via REST API)
2. Integrated using FHIR/HL7 (through the QHIE-Hub Platform)

Certain requirements (e.g., integration, historical data migration etc.) are different across the above methods and across entity types (e.g., hospital v/s pharmacy). Hence, based on the selected method, a healthcare provider or pharmacist must get familiar with and implement specific requirements that are applicable to them. The table below outlines all applicable chapters in the onboarding handbook and their corresponding requirements for different methods of access based on the entity.

For outpatients, a real-time integration needs to be done (i.e., their prescriptions/ dispensing information needs to be sent on a real time basis). However, for inpatients, prescription/ dispensing information can be sent upon discharge of the patient.

		Prescription		Dispensing	
	Mode of access	Standalone (including embedded option)	Integrated via FHIR/HL7	Standalone (including embedded option)	Integrated via FHIR/HL7
	Chapters	Healthcare providers who do not have FHIR/ HL7 integration capabilities	Healthcare providers who have an EMR (eRecords) or Basic EMR that integrates with Core	Healthcare providers and pharmacies who do not have FHIR/ HL7 integration capabilities & do not plan to integrate with Core	Healthcare providers and pharmacies integrating with Core
Section A: Get familiar with the QHIE-Hub	1. About the QHIE-Hub	Yes	Yes	Yes	Yes
	2. Accessing patient data (consent settings applicable to access prescriptions by other providers/pharmacists)	Yes	Yes	Yes	Yes
	3. Mandate, key policies & guidelines	Yes	Yes	Yes	Yes
Section B : Get ready to onboard	4. Your readiness journey	Yes (except connection to sandbox and development of APIs)	Yes	Yes (except connection to sandbox and development of APIs)	Yes
	5. People and support	Yes	Yes	Yes	Yes
	6.1 Security and connectivity via GN/ISP Hub	Yes (except connection to sandbox)	Yes	Yes (except connection to sandbox)	Yes
	6.2 Integration with QHIE-Hub Platform	No (direct integration with eMeds)	Yes	No (direct integration with eMeds)	Yes
	6.3 Data (use of QNDC for drugs, ICD10CM for diagnosis codes)	Yes	Yes	Yes (+ GTIN & Serial Number for drug tracking)	Yes (+ GTIN & Serial Number for drug tracking)
	7. Ready to onboard	Yes	Yes	Yes	Yes
	8.1 Connect to the QHIE-Hub Prod environment	Yes	Yes	Yes	Yes
	8.2 Execute historical data migration (after terminology mapping)	Active Prescription (including actively used drugs, partially dispensed / pending dispensing)	Active Prescription (including actively used drugs, partially dispensed / pending dispensing)	No	No
	8.3 Training	Yes	Yes	Yes	Yes
	8.4 Go live	Yes	Yes	Yes	Yes
Section C : After you onboard	9. What to expect after onboarding (adoption, release management, support & maintenance, security monitoring)	Yes	Yes	Yes	Yes
	10. Continuous governance	Yes	Yes	Yes	Yes

Table 7. Relevant onboarding handbook chapters for access methods for eMeds modules

The remaining section provides an overview of the access methods along with additional details healthcare providers and pharmacies must take note of.

1. **Standalone method**

    a. This method enables users to access the ePrescription and Pharmacy Network (eMeds) solution using internet access directly via a web-browser. All users/ entities will be able to use this method of access. Healthcare providers can use this method with or without Rest API, FHIR/ HL7 integration or the availability of an Integrated EMR solution (eRecords).

    b. Alternatively, the URL can also be embedded within the healthcare provider EMR or dispensing system via Rest API. In this case, eMeds gets an access token with healthcare provider client credential for opening the eMeds along with sign-in information of the practitioner along with patient information.

    c. **Users will have access to all the functionalities that are available to their role/entity** (i.e., prescribing, updating & canceling prescriptions, signing, co-signing for hospitals/practitioners (or) dispensing, returning, reporting adverse events, viewing medication history and medication list, and checking for interactions for pharmacists).

    d. The only requirement for this method is internet access, a compatible web browser (for website access) and the ability to configure Rest APIs (that generate "Bearer Token" for authorization and send a reference code request along with practitioner credentials and patient information)

    e. It is important to note that this method of using the eMeds solution requires a user to use two applications and requires a partial integration between them. However, embedding the application URL within the EMR/dispensing system and using access tokens is a simple and effective way to ensure a unified user experience. To elucidate:

        i. At the time of prescribing a drug, a physician needs to switch to the eMeds solution to write a prescription and then return to their EMR for other clinical processes. This prescription information needs to be sent back to the Hospital EMR via the QHIE-Hub Platform for completeness. (This is a default use case since all hospitals/ clinics need to integrate their EMR with the QHIE-Hub Platform or use the Basic EMR solution which is already integrated with the QHIE-Hub Platform). Healthcare providers can easily implement the embedded method to ensure physicians do not need to enter their credentials or patient information again, thereby creating a seamless user-experience.

        ii. On similar lines, at the time of dispensing a drug, a pharmacist needs to switch to the eMeds solution to dispense a prescription and then return to their dispensing system for other billing processes. The dispense information needs to be sent back to the dispensing system from the eMeds solution for completeness. Pharmacies can develop simple workflows that ensure pharmacists do not need to enter their credentials or prescription information within eMeds to create a unified, hassle-free experience.

2. **Healthcare provider to QHIE-Hub Platform Integrated FHIR/HL7 [Indirectly to eMeds]**

    a. This method involves fully integrating the healthcare provider EMR or dispensing system with the ePrescription and Pharmacy Network (eMeds) solution through QHIE-Hub Platform via FHIR/HL7 APIs.

    b. The advantage of this method is that users can access ePrescription and Pharmacy Network (eMeds) from within their existing systems (without switching applications) – making the overall experience seamless. Due to the full integration, the users can continue operating within their own systems without any need to switch to use the eMeds solution to prescribe or dispense medications. The interfaces will ensure that all information is shared, and all rules are validated.

c. However, this method limits the functionality available to users.

- Management module is not available to users
- Prescribing module features such as co-sign and viewing medical history are not available to physicians
- Dispensing module features such as renewal, digitization of prescriptions, viewing medical history or interaction lists are not available to pharmacist

This method is suitable for healthcare providers who have FHIR/HL7 integration capabilities and plan to integrate with QHIE-Hub Platform. The requirements for this method include availability of FHIR/HL7-based integration capabilities within the EMR and the ability to configure FHIR/HL7 APIs. Detailed information is available in the interface specification documents shared as part of the onboarding resources.

6.4.4 Business workflows

As part of onboarding to the ePrescription and Pharmacy Network (eMeds) solution, there are multiple business workflows that healthcare providers must implement based on their access method. These are provided in the Future state workflows document as part of the onboarding resources. Healthcare providers are expected to go through these workflows along with other resources like interface specifications and make the required changes to their EMR/dispensing systems.

Additional guidelines regarding prescription, dispensing, drug rules and restrictions with be published by MoPH in due course of time. Healthcare providers must familiarize themselves with these guidelines and implement them.

*****

CHAPTER 6.5

National clinical viewer (eConnect)

This section is intended to guide healthcare providers and pharmacies as they get onboarded to the **National clinical viewer (eConnect)**. It provides an overview of the features of the solution, different methods to access it and outlines requirements that are specific to the method of access chosen by the healthcare provider.

6.5.1 Overview of the solution

The **National clinical viewer (eConnect)** is a national solution that gives healthcare professionals access to the patient's longitudinal health records under a specific consent management workflow. It is designed as a view-only platform based on data from the QHIE-Hub collected from the hospital EMRs, pharmacies and the Personal Health Record solution.

Once a healthcare provider logs into the solution and has obtained access to the patient record (based on patient consent settings), they can access the following modules/pages (as shown in the figure 28. and outlined below):

1. **Patient Profile:** Displays general patient information such as name, date of birth, nationality, QID, NHN number etc.
2. **Patient Summary:** Displays the patient's clinical history information, giving a summary of each module.
3. **Encounter Summary:** Displays the encounter information available in a list view and gives the user the ability to perform actions such as searching encounters or viewing details of encounters
4. **Allergies and Intolerances:** Displays specified allergy and intolerances information

National clinical viewer (eConnect) will provide users with 360 degrees view of clinical data, from all facilities in Qatar

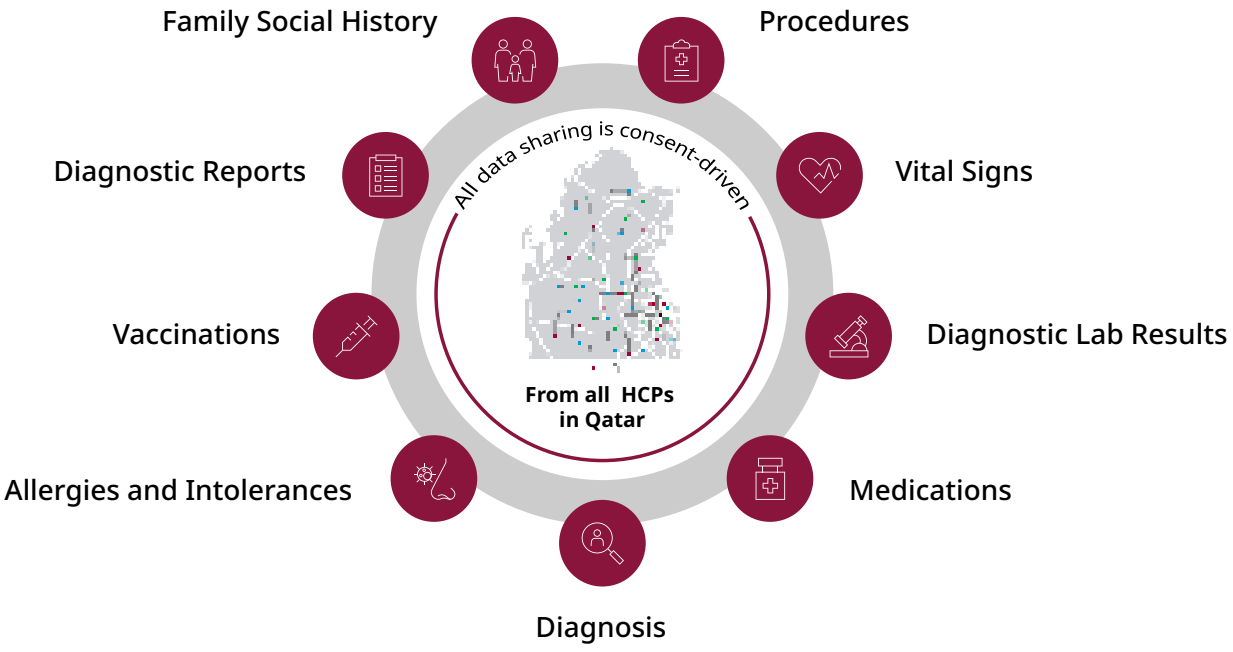


Figure 28. Overview of eConnect features

5. **Care Plans:** Displays care plan information in a list view
6. **Clinical Documents:** Displays clinical documents available within the QHIE-Hub for a patient in a list view and allows the practitioner to view related reports
7. **Diagnoses:** Displays specified diagnoses in a list view
8. **Diagnostic Laboratory Tests:** Displays laboratory information in a list view
9. **Diagnostic Reports:** Displays diagnostic reports information in a list view and allows the practitioner to view the related report of each procedure (if available)
10. **Family and Social History:** Displays family and social history information in a list view
11. **Medications:** Displays medications information in a list view
12. **Patient Added Information:** Displays information provided by the patient from their Personal Health Record
13. **Procedures:** Displays medical procedures carried out on the patient and allows the user to view related reports of each procedure (if available)
14. **Vaccinations:** displays specified vaccinations information categorized into routine pediatric, routine adult and other vaccines; also displays specified vaccines as a schedule for pediatric patients, highlighting the vaccines that have been administered, overdue or approaching are approaching

Vital Signs: Displays vital signs information, separated into inpatient and outpatient, giving the user the ability to perform actions such as sorting and filtering the information displayed

6.5.2 Access methods

Access and integration to the National clinical viewer (eConnect) is achievable through two methods. The choice of method depends on the nature of the entity, preference, and technical capabilities.

The two methods include:

1. Standalone
2. Embedded using Rest API

National clinical viewer (eConnect) can be accessed using two methods: Standalone and Embedded using Rest APIs. Standalone can be used by all stakeholders whereas embedded can be used by HCPs using EMR.

Figure 29. is a detailed description of National clinical viewer access methods

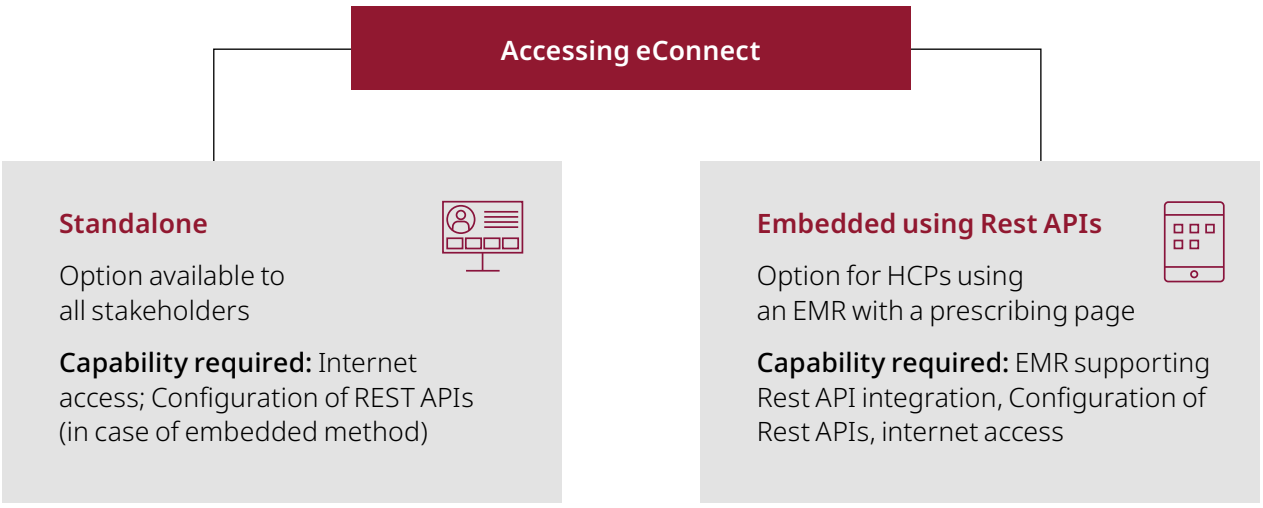


Figure 29. Methods to access National clinical viewer (eConnect)

1. **Standalone method**

   a. This method enables users to access the National clinical viewer (eConnect) using internet access directly via a web-browser. All users/entities will be able to use this method of access. Healthcare providers can use this method without a need for FHIR/HL7 integration with QHIE-Hub Platform or an EMR.

   b. Users will have access to all the functionalities required for their role/ entity (e.g., Accessing Patient Medical records, viewing encounters, Allergies, Observations, Procedures, etc. for hospitals/practitioners. However, users will be required to login through credentials every time they access National clinical viewer in standalone mode.

   c. The only requirement for this method is internet access and a compatible web browser.

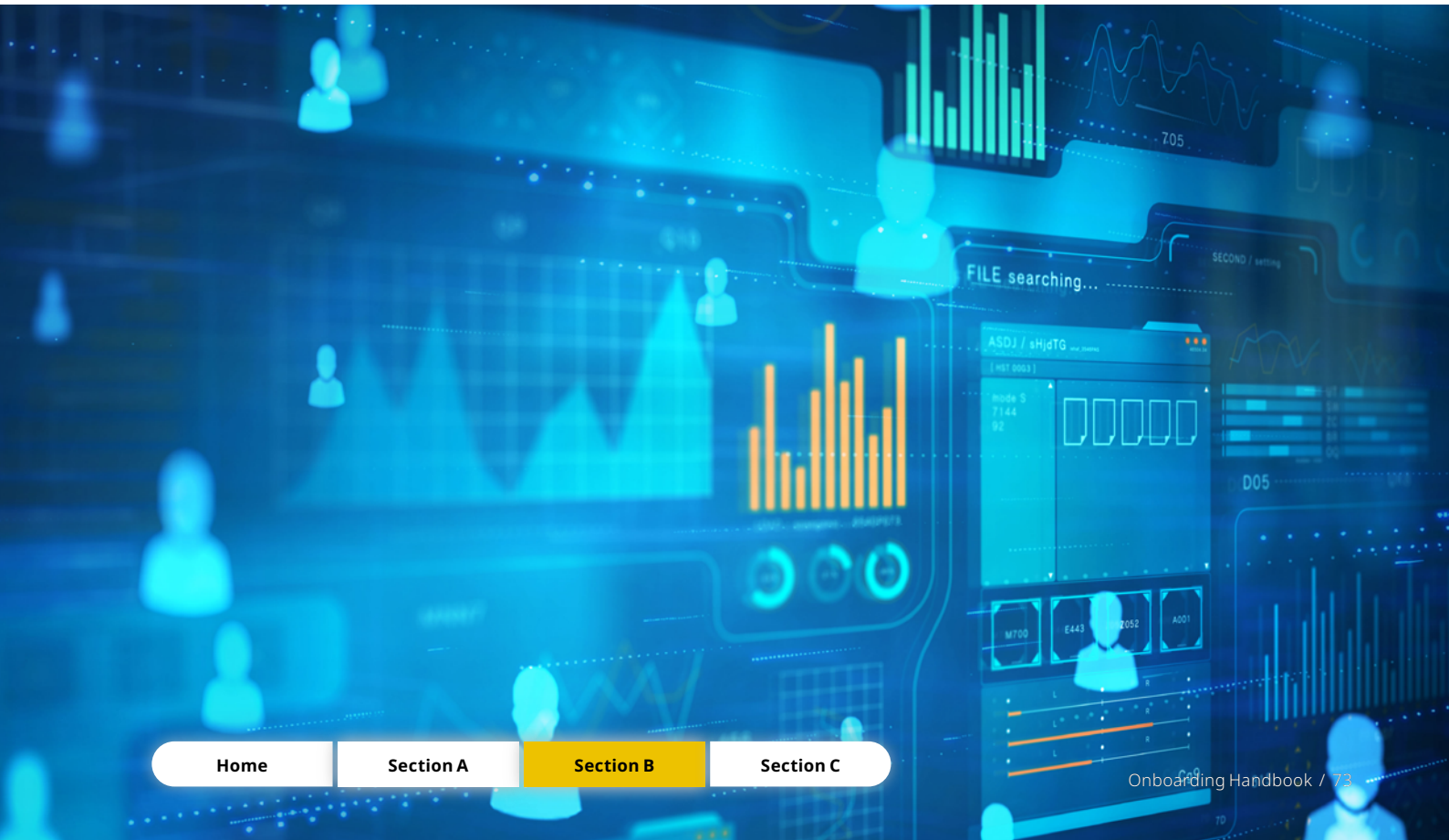
2. **Embedded using Rest API**

   a. This method enables users to reach the landing page of the National clinical viewer using API services.

   b. Users will have access to the full services of Health Information Exchange like the standalone method. The advantage of this method is that the user login credentials, and patient information are sent from the healthcare provider's EMR to the Health Information Exchange using APIs – making the experience seamless for users by enabling auto login & autofill of patient information.

This method is suitable for healthcare providers who have an EMR and possess API integration capabilities. The requirements for this method include the ability to configure and use Rest APIs.

*****



CHAPTER 6.6

Registries and care plans (eCare)

This section is intended to guide healthcare providers as they get onboarded to the **Registries and care plans (eCare)** solution. It provides an overview of the features of the solution, different methods to access it and outlines requirements that are specific to the solution beyond requirements laid out in the previous sections.

6.6.1 Overview of the solution

Registries and care plans (eCare) solution serves as an all-in-one platform for care plans, national registries, and statistics for the management of the targeted chronic disease and conditions. eCare is designed to establish nationwide registries for targeted diseases and conditions and help standardize patient care through personalized care plans based on national clinical guidelines.

eCare solution enables healthcare providers to track patients treated in their organizations through local disease registries (i.e., disease registry lists created from information of these patients). It provides them with comprehensive reports and statistics to identify disease trends and track disease progression generated from their patient population enrolled in the registry.

The solution also streamlines care coordination by allowing members of the care team to communicate with each other and provides them with comprehensive reports and statistics to identify disease trends and track disease progression on a single platform.

As outlined earlier in the document (in Section A), Registries and care plans (eCare) solution consists of care plan and registry, and reports and statistics modules. Details on each module are provided in their respective section as follows:

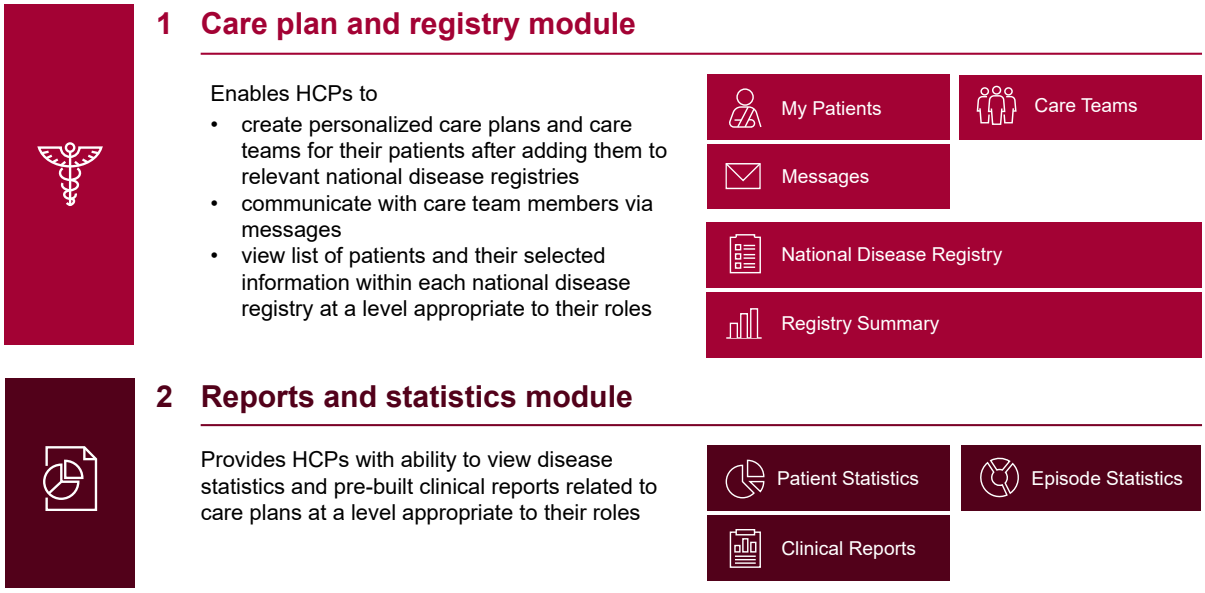


Figure 30. Overview of Registries and care plans (eCare) modules and features within each module

1. Care Plan and Registry Module

The Care Plan and Registry Module in the eCare solution is designed to facilitate evidence-based decision-making in chronic disease and condition management. This module offers a range of features for personalized care planning and care coordination for patients in national disease registries.

Healthcare professionals are required to add their patients to national disease registries relevant to their diseases and/conditions before using the care plan functionality for these patients.

eCare solution uses the Enterprise Master Patient Index (eMPI) service to add patients to registries. Healthcare providers can search for patients using the eMPI services of the QHIE-Hub and manually add patients to registries relevant to their diseases and/or conditions. Details for this service are provided in section 6.6.5.

This module has five sub-sections, and each sub-section is described in detail below.

1.1 My Patients

This section allows physicians and allied healthcare professionals with full access to start or continue a care plan or a follow-up episode for their patients. In each episode, practitioners select risk factors and examination findings. Registries and care plans (eCare) solution analyzes these inputs along with clinical information (e.g., medications, lab investigations) pre-populated from the QHIE-Hub platform and generates recommendations aligned with the national clinical guidelines. For this analysis to happen, users must provide inputs for all mandatory fields (e.g., diagnosis). Following the recommended interventions, which may include medications, labs, treatment goals, educational materials, and referrals, providers can create personalized care plans for their patients.

Select details from personalized care plans such as educational materials and treatment/ lifestyle management goals recommended by practitioners are shared with patients through the Personal Health Record (PHR App) solution through the QHIE-Hub platform.

All users, irrespective of their access level (full access or read-only), can view summaries of previously created care plans and episode history for each patient through **patient dashboard (Figure 32).**

Additionally, physicians can also view detailed care plans for individual patients on National clinical viewer (eConnect) by using the eConnect button located in episodes and patient dashboard. This feature is available to all physicians, regardless of their access level.

This section also enables Registries and Care plans (eCare) users with full access to manually add or remove patients to/from a registry. To remove a patient, a removal reason must be selected. However, users with read-only access are not permitted to use the removal feature.

Registries and care plans (eCare) solution obtains clinical information required for care plans, such as vital signs, current medications, and lab test

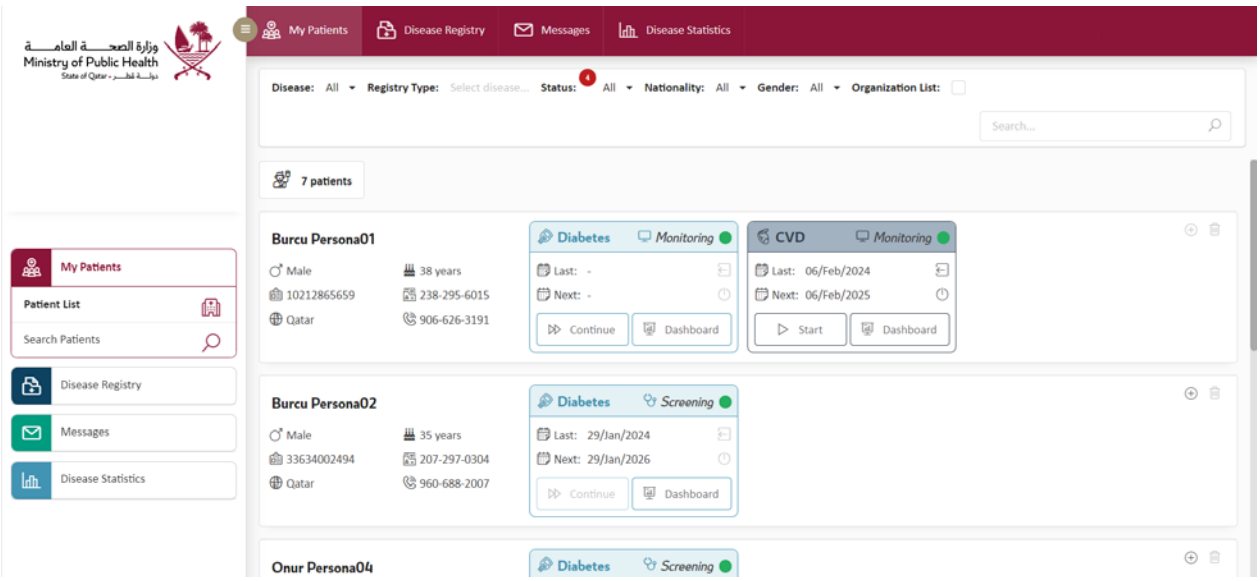


Figure 31. My Patients Page

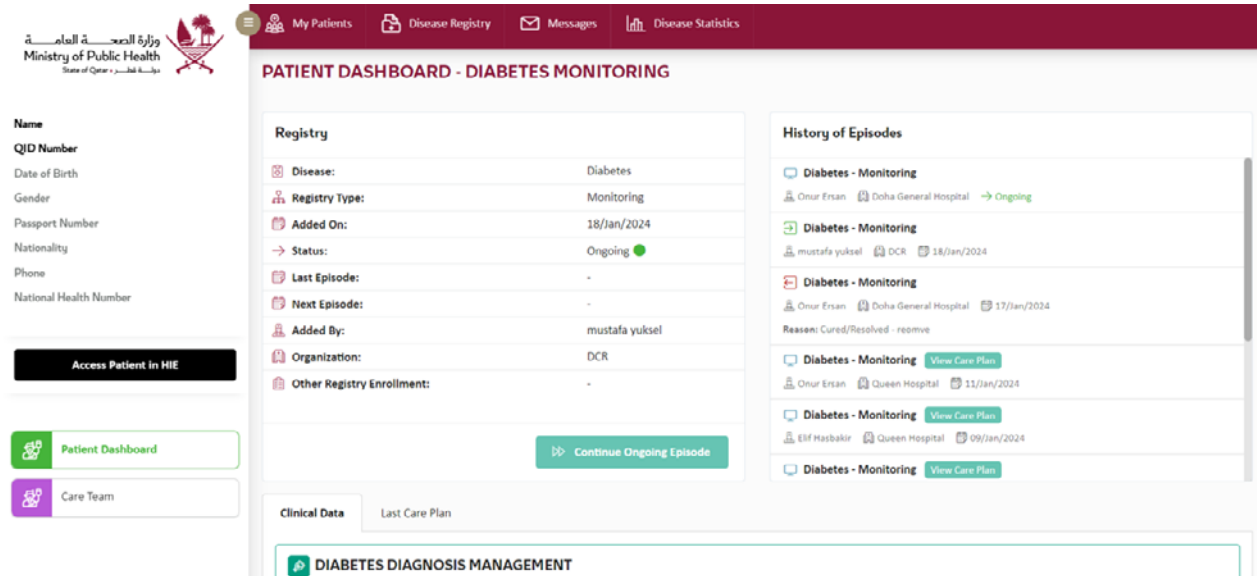


Figure 32. Patient Dashboard

results, from the QHIE-Hub platform. It sends back certain orders recommended by the practitioner (i.e., medications, lab tests, referrals) to the healthcare provider's EMR through the QHIE-Hub platform. Therefore, integration of provider's EMR and QHIE-Hub platform is necessary to effectively use the care plan module of eCare. Further details are provided in Section 6.6.4.

1.2 Care Teams

This section allows eCare users to view members within each patient's care team and perform certain operative tasks allowed as per their role(s) and access level(s).

All users, irrespective of their access level, can view care team members for an individual, and all users, except heads of healthcare facilities, are allowed to remove a member from the care team. Only physicians with full access and heads of clinical departments are permitted to add a healthcare professional to the care teams.

1.3 Messages

This section enables eCare (Registries and care plan) users to send and receive messages to/ from care team members, either individually or collectively, and individually from patients.

The sole purpose of the message functionality is to enhance communication between care team members, and physicians and their patients on topics related to clinical care of the patients. Therefore, users should not use this section to engage in personal conversations with their colleagues/patients or share any PHI/PII information of their patients.

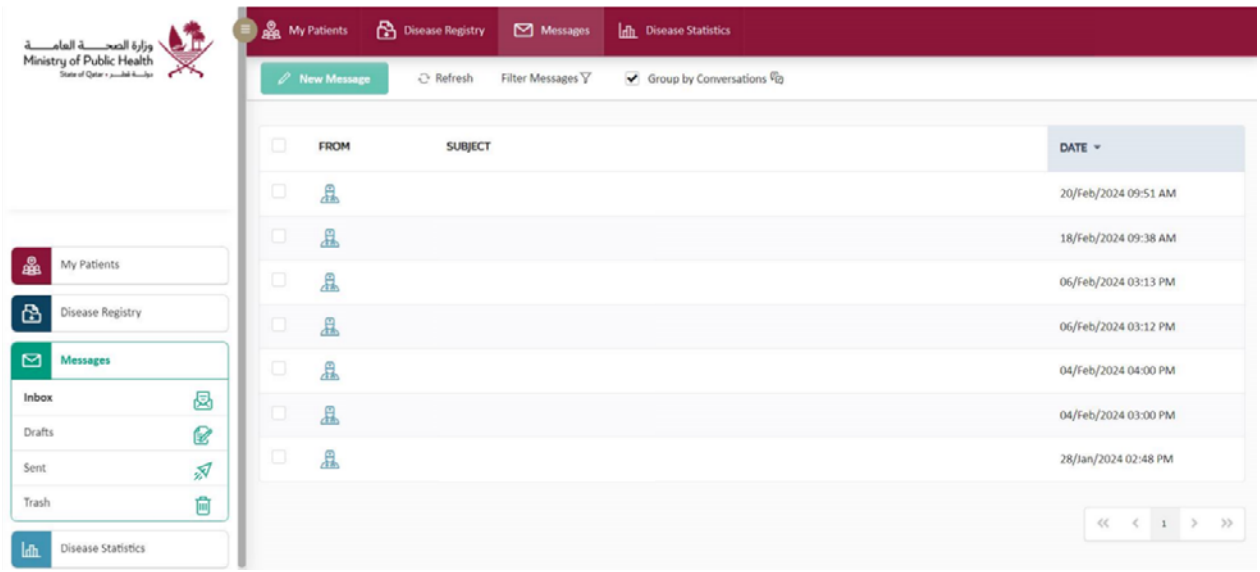


Figure 33. Messages

Users can perform following actions in the inbox, drafts, sent, and trash sub-sections of the messages section:

- Read messages they receive
- Send new messages with or without attachments
- Filter messages by message content
- Organize their received messages by grouping them by conversations (i.e., messages from same individuals or care teams are considered part of a conversation)
- View and edit messages they have created but not sent yet
- View messages they previously sent
- View messages they deleted and remove these from their trash

Once a message is sent to a healthcare professional, recipient sees a red icon next to in the messages title both on the left side and at top of their screen when they log into the eCare solution. If a message is sent to a patient, recipient sees a notification for the message when they log into the Personal Health Record solution.

All eCare (Registries and care plans) users, except heads of healthcare facilities, are allowed to send messages to healthcare professionals within the care teams and patients through this section.

1.4 National Disease Registry

This section includes national disease registries, which are organized systems for collecting, storing, and managing clinical data related to patients with target chronic diseases and/or conditions across the nation. This module is designed to enable better understanding and management of different types of target diseases and/or conditions.

This section displays the list of patients and their selected information within each disease registry.

The information shown in the list includes name, QID, gender, birth date, age, nationality, phone number, diagnosis, diagnosis code, diagnosis date, city, physician, organization, registry status (i.e. active/inactive), registry entry date, level of care (i.e., A, B and C; based upon the number of complications), disease control (i.e. Adequate, Optimum, and Uncontrolled) number of episodes, and last episode date, for each patient in the selected registry.

As of now, eCare solution only has the national disease registry for diabetes mellitus (DM), focusing on type 1 DM, type 2 DM, gestational DM, and pre-diabetes (Figure 40). Cardiovascular Disease (CVD) registry focusing on hypertension, angina, myocardial infarction, coronary syndrome will be launched in 2024 and be immediately accessible to healthcare professionals with relevant roles. Registries

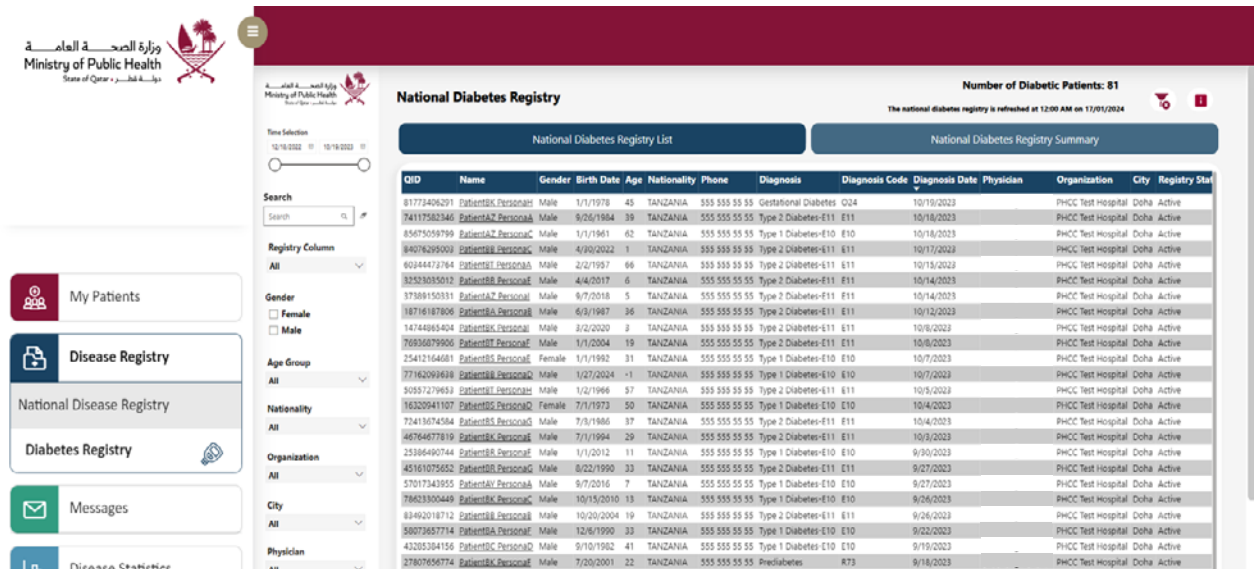


Figure 34. National Diabetes Registry

for other selected diseases and conditions are planned to be launched in the near future.

Only physicians with full access, heads of clinical departments, and heads of healthcare facilities are allowed to view the national disease registries and their summaries. However, the level of information displayed is based on their roles. Physicians only have access to the information of their patients, heads of clinical departments have only access to the information of patients treated in their departments, and heads of healthcare facilities only have access to the information of patients treated in their facilities.

Users with access to a registry can search patients (as per their access level) by their QIDs and use filter options to view only sub-sets of the registry. They can also export the registry list as an Excel file. If allowed by their rights, a user can view the care plans of a patient in the list by clicking on their name, which opens the patient dashboard of the respective patient.

All information displayed in the National Disease Registry is read-only and controlled by the Ministry of Public Health (MoPH) admins. However, healthcare providers can contribute to the national disease registries by keeping patients' clinical information up to date in their EMR and through care plans designed via eCare (Registries and care plans) solution, and also by manually adding their patients with target chronic diseases and/or conditions to relevant national disease registries (Section 6.6.5).

All healthcare providers must migrate their existing registries to the eCare solution during the QHIE-Hub onboarding process (Section 6.6.5), which is essential for the comprehensiveness and accuracy of the national disease registries.

1.5 National Disease Registry Summary

This section displays the summary for each disease registry through graphs and epidemiological statistics (e.g., prevalence and incidence of diabetes mellitus).

Graphs and statistics provided in this section are read-only and controlled by the Ministry of Public Health (MoPH) admins.

2. Reports and Statistics Module

The Reports and Statistics Module of the Registries and Care plans (eCare) solution includes the statistics and clinical reports generated from the data of patients within each disease registry.

Statistics and reports provided in this section are read-only and controlled by the Ministry of Public Health (MoPH) admins.

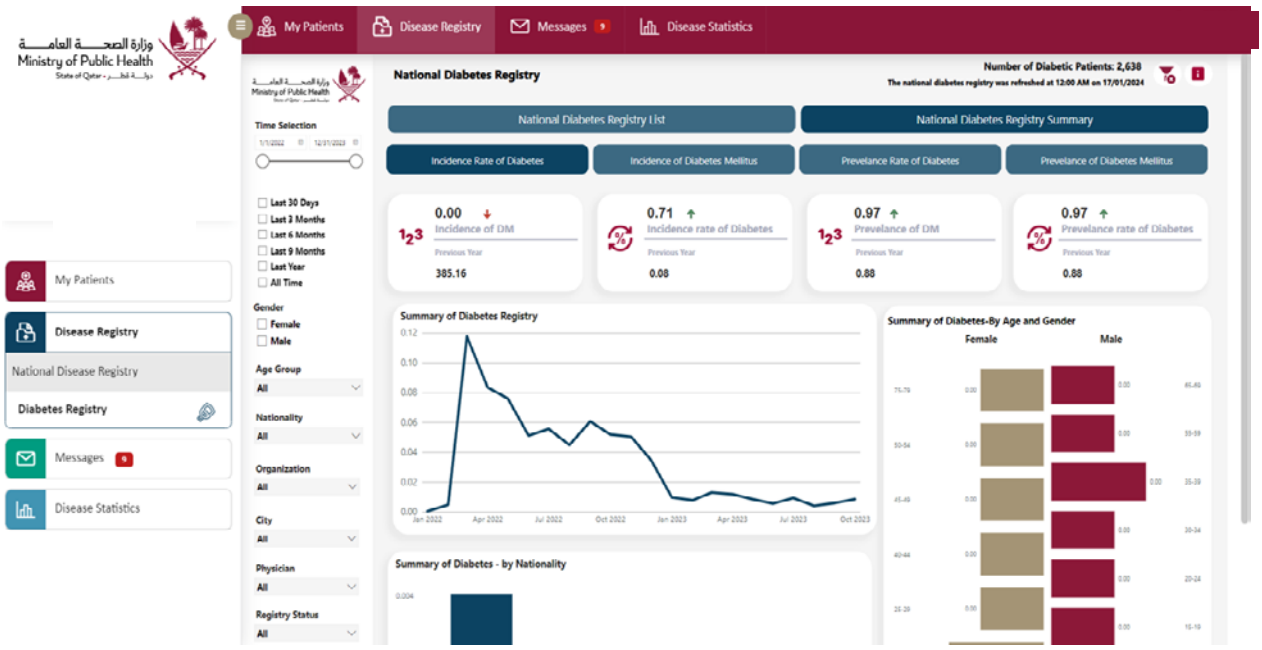


Figure 35. Registry Summary

Only physicians with full access, heads of clinical departments, and heads of healthcare facilities are allowed to view the patient statistics, episode statistics, and clinical reports in this module. However, the data used to generate statistics and clinical reports is based on user's roles. Only MoPH users or users provided national level access can access reports and statistical analysis from country level data.

Physicians with full access are permitted to see statistics and reports for their patients. Heads of clinical departments are allowed to see statistics and reports for their patients and for the patients treated in their departments. Heads of healthcare facilities are only able to see statistics and reports for the patients under their personal care and those being treated in their facility.

The Disease Statistics Module is designed to provide insights into disease trends and management across different patient groups through three sections.

2.1 Patient Statistics

This section includes pie charts and scorecards displaying the number of patients by their status for each disease registry.

There are 4 possible statuses in the National Diabetes Registry such as previously followed, ongoing, on-hold, and initial visit pending.

Users are allowed to filter these statistical data by disease registry (e.g., diabetes), nationality, gender, age, and a date range.

These pie charts allow users to track patients by their status in the disease management process and identify patterns, such as frequent or delayed status changes, which may signal areas needing improvement in patient management.

2.2 Episode Statistics

This section includes pie charts and scorecards displaying the number of episodes by their status for each disease registry.

There are 4 possible statuses the National Diabetes Registry such as completed, ongoing, on-hold, and cancelled.

Users are allowed to filter these statistical data by disease registry (e.g., diabetes), nationality, gender, age, and a date range.

These pie charts allow users to track the changes in episode status to improve care delivery and compliance with treatment plans.

2.3 Clinical Reports

This section provides in-depth clinical reports generated from the patient data in each national disease registry, aiding in targeted analysis and research.

Each national disease registry has its own set of comprehensive reports, tailored according to the healthcare needs, standard of care and the national clinical guidelines. Consequently, reports available for each registry may vary.

eCare (Registries and care plans) solution has the following clinical reports for the national diabetes registry (Figure 36):

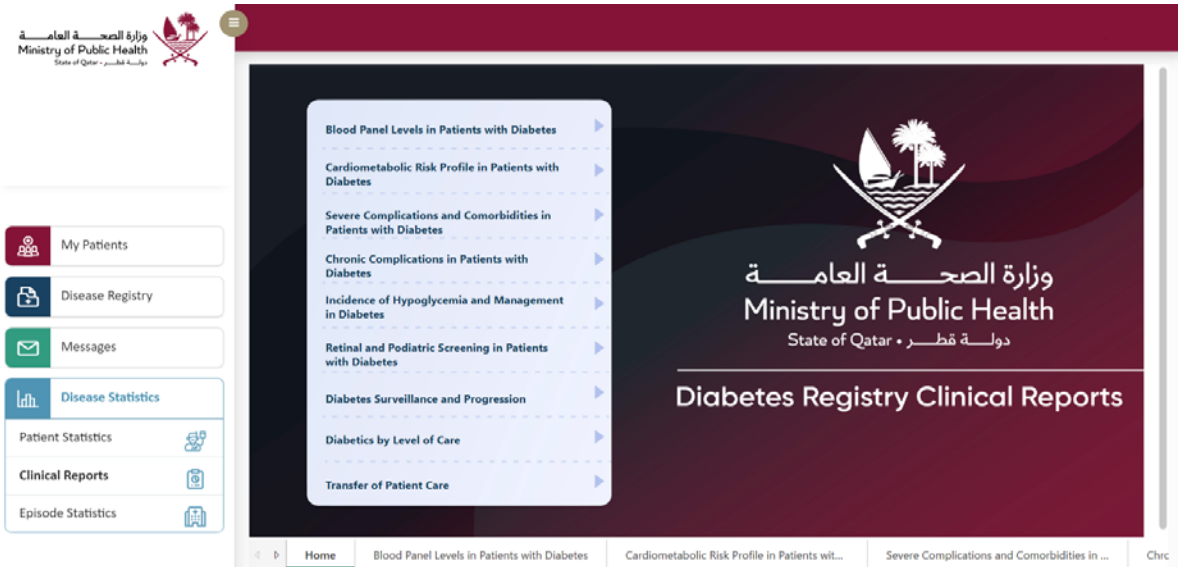


Figure 36. Diabetes Registry Clinical Reports Home Page

- Blood Panel Levels in Patients with Diabetes
- Cardiometabolic Risk Profile in Patients with Diabetes
- Severe Complications and Comorbidities in Patients with Diabetes
- Chronic Complications in Patients with Diabetes
- Hypoglycemia Incidence and Its Management in Patients with Diabetes
- Retinal and Podiatric Screening in Patients with Diabetes
- Diabetes Surveillance and Progression
- Diabetic Patients by Level of Care
- Transfer of Patient Care

Users are allowed to filter the data in reports by date, gender, age, nationality, and organization and also export the clinical reports. However, they cannot generate custom reports in this section.

6.6.2 Consent settings

The **Registries and care plans (eCare)** solution follows the standard consent management workflows within the QHIE-Hub. Patient consent will be required to grant a healthcare practitioner the permission to view clinical information of the patient and subsequently to create care plans. The default setting enables sharing of clinical data with healthcare providers for all patients. However, patients have the option to change these settings at any time through their Personal Health Record profile.

Certain functionalities of the solution such as generating reports or accessing care team information will not require patient consent.

6.6.3 Access methods and privileges

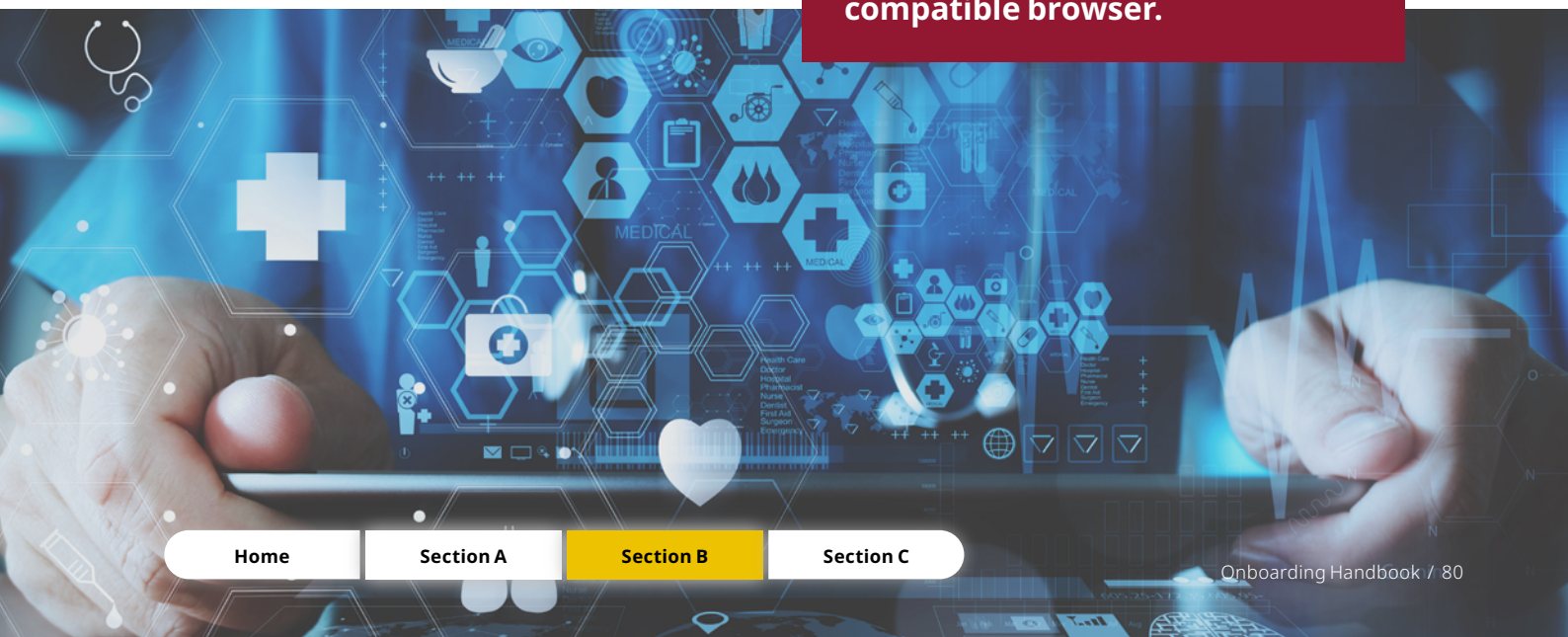
The Registries and care plans (eCare) solution is a web-based application, which can be accessed in a standalone manner only via a web browser. The only requirement to access the solution is internet access with a compatible web browser.

Care plans from the Registries and care plans (eCare) solution will be available on the Health Information Exchange (HIE) solution both via the standalone and integrated method. In the integrated method (i.e., via HIE), healthcare professionals will be able to view care plan summary of a patient but will be unable to use other functionalities of the eCare solution in this method.

Users will have access to eCare features based on their role (i.e., creating and managing care plans, accessing data and reports within the eCare registries). Features available by user role are outlined in **Table 8**.

Level of access (i.e., full, read-only) to the Registries and care plans (eCare) solution will be determined by the practice scope of the healthcare professionals and its relevancy to a national disease registry. For example, a cardiologist will be given read-only access to the national diabetes registry and full access to the national cardiovascular disease registry.

eCare can be accessed using the standalone method, requiring only internet access with a compatible browser.



At the time of onboarding to the Registries and care plans (eCare) solution, healthcare professionals and their roles will be verified with details from the Department of Healthcare Professionals (DHP). After the verification, they will be provided with the level of access that is relevant to their scope of practice.

Feature	User role					
	Physician with full access	Physicians with read-only access	Associate medical role with full access	Associate medical role with read-only access	Head of a clinical department	Head of a healthcare facility
Start or continue a care plan	X		X			
Review previously created care plans	X	X	X	X	X	X
Add a patient to a disease registry	X		X			
Remove a patient from a disease registry	X					
Add a member to a care team	X				X	
Remove a member from a care team	X	X	X	X	X	
Send and receive messages from/to care team members	X	X	X	X	X	
View and filter disease registries	X	X	X	X	X	X
View and filter reports and statistics	X				X	X

Table 8. Features available by user role

6.6.4 Dependency on real time integration of HCPs to the QHIE-Hub

The Registries and care plans (eCare) utilizes clinical information collected through EMRs (e.g., vital signs, lab test results) and retrieve all relevant information from the QHIE-Hub platform. Therefore, a real-time integration between the healthcare provider's EMR to the QHIE-Hub platform is necessary to ensure:

- Disease and condition registries are auto populated with latest patients who are under a provider's care
- Care plans are tailored to the most recent clinical data of patients
- Reports are generated using the up-to-date clinical data
- Recommendations in care plans are shown on healthcare provider's EMR interface

6.6.5 Population of the registries

The Registries and care plans (eCare) solution stores the demographic data of patients belonging to a specific registry along with their care plan information. However, all the clinical data in this solution will be sourced from the QHIE-Hub platform (i.e., Core solution) to ensure care plan management is done based on the most recent clinical data of patients. Therefore, onboarding and real-time integration with the QHIE-Hub platform is necessary before a healthcare provider can proceed to get onboarded to the eCare solution.

As part of their onboarding to the National Clinical Viewer (eConnect)and eMeds solutions, healthcare providers would have shared all the historical data of their patients (e.g., type, condition, stage) via either interface loads (i.e., FHIR R4B or HL7 v2.5.1) or via the CSV method and have completed their integration into the QHIE-Hub platform. After this activity, level of work required to meet pre-requisites for Registries and care plans (eCare) onboarding process is considerably less due to the commonalities between onboarding activities for the HIE, eMeds, and Registries and Care plans (eCare) solutions.

To be onboarded to the Registries and care plans (eCare)solution, healthcare providers should upload their internal registry data containing the details about the patients for different diseases and conditions, if available and applicable. This is required by Ministry of Public Health and included in the MoPH QHIE-Hub Mandate to ensure that national disease registries contain the records of all patients with targeted disease and/or conditions.

During the onboarding process to the eCare solution, data migration activity a healthcare provider needs to undertake is to add the list of patients belonging to a specific registry at their end. This could be done via manual search or bulk-upload options outlined below.

Population of national disease registries in the Registries and care plans (eCare) solution is done through three ways:

1. **A manual search and entry of patients within the Registries and care plans (eCare) solution**
2. **A bulk-upload using the pre-defined CSV templates**
3. **Automatic selection based on the pre-defined criteria**

The following section describes these three options.

1. Manual Registration

Healthcare providers that do not have existing registries or have a limited number of patients have the option to enroll their patients manually to the respective registry in the eCare solution by searching and adding the patient via the eMPI service of the QHIE-Hub platform. However, healthcare providers will only be able to add the patients that have previous or ongoing encounters within their facility to the relevant registries (e.g., patient with type 2 diabetes mellitus should be added to the diabetes registry).

Healthcare providers can manually assign the patient to the disease registry in the care plan sub-module. However, scanning of documents will not be allowed, to prevent inconsistencies in data entry.

2. CSV Upload

An alternative approach available to healthcare providers is to add patient lists into the eCare solution by using the CSV upload option that supports bulk enrolment of patients. However, a healthcare provider will be responsible to ensure that only those patients who meet the requirements set forth in the national clinical

guidelines for inclusion in a specific registry are added. To use this approach, it is important for healthcare providers to meet the below pre-requisites:

- Populate the patient data as per the eCare CSV template (available as part of the onboarding resources)
- Name the file as per the applicable naming convention
- Ensure that the prescribed business rules are followed for all fields
- Validate all patient demographic data using the eMPI tool

Once a healthcare provider has completed the above pre-requisites, they must share the results from the final output of the eMPI tool with their facility manager for validation. An approval from the facility manager must be taken to upload the CSV file into facility's Azure Storage account, which will be provided during the Core onboarding process. This tool will check for the compliance of the uploaded files with pre-defined target datasets and business rules for each element and generate a report highlighting errors, if any.

No troubleshooting support will be provided to the healthcare providers who upload registry data directly without completing the pre-requisites or without securing an approval from their facility manager(s).

Applicable Naming Convention to be followed for eCare-specific CSV files:

As outlined in Section 8.2, healthcare providers must follow the naming conventions stated below when uploading CSV files into into the Azure Explorer tool to cleanse data using the data quality and eMPI tools. Files which are not compatible with this naming conventions, will not be uploaded to the system. The name of CSV file must be **r'^ RESOURCENAME_\d{8}_.*_eCare\.csv$'**. The only modification made to the current naming convention is that a healthcare provider must add **_eCare** with their entity name as part of the .* string, as highlighted in red.

The table 9 shows a sample CSV name that HCP1 plans to upload in the eMPI tool ahead of Registries and care plans (eCare) data migration on 13 July 2023.

3. Automatic

Registries and care plans (eCare) solution automatically enrolls patients who meet pre-defined criteria based on the national clinical guidelines into relevant disease and condition registries.

Once the integration between HCP's EMR and QHIE-Hub is established, the system analyzes patient data from the HCP to identify patients that fit the diagnosis and/or screening criteria for targeted diseases and conditions. When a patient's medical information, such as diagnosis, treatment history, or lab results, aligns with the diagnosis or screening criteria for a disease or condition as outlined in the national clinical guidelines, the system automatically adds this patient to the relevant registry with their respective disease state (i.e., monitoring, screening).

Healthcare providers can change the disease state of a patient or remove the patient from a registry based on their up-to-date clinical evaluation and relevant lab tests mentioned in the national clinical guidelines after selecting a removal reason.

EXAMPLE NAMING CONVENTIONS
PATIENT_20230713_HCP1_.CSV

Table 9. Sample CSV file names for 13th July 2023


Mandate, policies &guidelines
Overview of national solutions
A. Get familiar with QHIE Hub
B. Get ready to onboard
Onboarding Roadmap
Implementation Plan
Change management
Meet requirements (security, integration, data)
Connect to sandbox to develop APIs
Map & transform data
Clean historical data
You are here
Validate patient demographics
Connect to Pre-prod to test workflows
Training
Complete onboarding assessment
Actual onboarding/production
Go live
GO LIVE
C. After you onboard
Drive adoption
Monitor data quality

CHAPTER 7

Ready to onboard

7.1 Test workflows in pre-prod

Connecting to Pre-Prod Environment

- After developing messages based on standards and successfully validating them in the QHIE-Hub sandbox environment, healthcare providers need to connect to the Pre-Prod environment provided by MoPH to test the business workflows using these APIs.
- To achieve the above, a healthcare provider will need to reconfigure the API endpoint to point (from Sandbox) to the QHIE-Hub Pre-Prod Environment and initiate testing using synthetic data.
- Healthcare providers are expected to log all changes made in their configuration from the QHIE-HUB sandbox to Pre-Prod. This can help mitigate potential issues and expedite connecting to the QHIE-Hub Prod environment.

This section outlines key steps in executing integration testing. It is assumed that all other testing types (e.g., unit and functional testing) have been performed by healthcare providers at their end.

HCPs need to connect the pre-production environment to test the business workflows using the APIs.The aim here is to develop, establish and maintain a consistent and automated process to build and test applications that will ensure reliability of the systems.

The purpose of this testing is to enable healthcare providers test integration with QHIE-Hub across all layers – network, data, and applications for all solutions i.e., the QHIE-Hub Platform, ePrescription and Pharmacy Network and Health Information Exchange. The outcome of this testing is to ensure seamless integration is established and there are no faults in connectivity, exchanging data or application workflows.

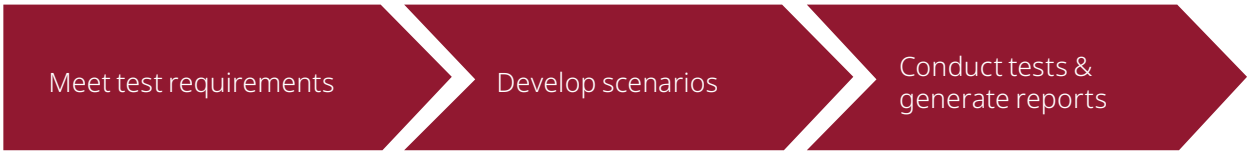


Figure 37. Steps to test workflows in Pre-prod

1. Meet test requirements

To start integration testing, healthcare providers must comply with the below prerequisites:

- Healthcare providers must provide their Facility license number to their Facility Manager to start the registration process of the HCP Client
- MoPH must register API clients on behalf of the healthcare provider to obtain a Client ID, Secret which will be used to generate JSON Web Token to enable secure data exchange.
- Network connectivity must be established with the QHIE-Hub according to the options described in Chapter 6.1.2 Network Connectivity.
- A secure staging (non-production) environment must be available at the healthcare provider's end
- APIs must be developed according to the Integration specifications shared along with the onboarding resources
- Business and technical workflows within provider EMRs or Prescription/dispensing modules must be developed according to the workflows outlined within the integration specifications
- Healthcare providers must generate and use synthetic/test data for test execution. They should not use actual patient data for testing purposes in the Pre-Prod environment to ensure patient privacy. To the extent possible, this test data must resemble the actual data generated by the healthcare provider (e.g., using the same code sets, systems, rules).
- Healthcare providers must ensure that patient names in the test data are created using the following naming convention for easy identification of the facility via Health Information Exchange.

  "FIRST NAME" "MIDDLE NAME" "HCP INITIALS (as last name)"

  - HCP INITIALS: First 4 letters of the healthcare provider's actual name (e.g., if the name of the patient is JOHN SMITH DOE and the healthcare provider is Contoso Hospital, then the patient's name will be **JOHN SMITH CONT**)
- Healthcare providers must inform their Facility Manager when they are ready with the test data to schedule a testing window.
- The Facility Manager must schedule the testing for the healthcare provider in the next available slot after receiving a request and must share the scheduling confirmation. Healthcare providers must prevent sending / sharing test data with the QHIE-Hub, unless previously planned and agreed with their facility manager

Note: Healthcare providers are expected to conduct testing using their own applications apps (eRecords, Prescription module, etc.) and are advised not to use any simulation tools (e.g., Postman, SOAP-UI, etc.)

2. Develop test scenarios

Integration testing must cover the following modules/specification types across the QHIE-Hub Platform, ePrescription and Pharmacy Network, Health Information Exchange solutions:

- eMPI
- Terminology management portal
- FHIR
- HL7 v2
- eMeds FHIR APIs
- eMeds Embedded
- National Clinical Viewer (eConnect) Embedded Viewer

This section covers the minimum recommended test scenarios and cases that healthcare providers are expected to execute. However, healthcare providers are expected to create and test additional scenarios based on their business workflows for a successful integration with the QHIE-Hub and to avoid any disruption to the healthcare provider operations within their facility due to this new national integration.

At a minimum, healthcare providers must perform the recommended scenarios for integration testing across all the modules of the QHIE-Hub platform. They are also expected to create additional scenarios based on their business workflows.

A. Access by using Login Credentials:

Test Case ID	Test Scenario Name	Test Scenario Description	Expected results
1.	General	Login to the application (eConnect/eMeds/eCare)	Should be able to Login directly to the application with the User credentials details created for the specific user

Table 10. Sample test scenario - general

B. Access by using Bearer tokens:

Test Case ID	Test Scenario Name	Test Scenario Description	Expected results
1.	General	Accessing with access token	"Bearer Token" for authorization should get added successfully

Table 11. Sample test scenario - access token

Bearer tokens to be obtained for sharing data with the QHIE-Hub platform via FHIR, HL7v2, APIs etc.

C. eMPI (Enterprise Master Patient Index)

Test Case ID	Test Scenario Name	Test Scenario Description	Expected results
1.	Create	Create Unknown Patients	Successfully create Unknown Patients
		Create Patient with Identifier	Successfully create Patient with Identifier
		Create Newborn Patients	Successfully create Newborn Patients
2.	Query	Query patient from eMPI	Successfully query patient from eMPI
3.	Retrieve	Retrieve patient from eMPI	Successfully retrieve patient from eMPI
4.	Merge	Test Merging patient records	Successfully merge patient records
5.	Unmerge	Test Unmerge for merged patients	Successfully Unmerge the merged patients
6.	Update	Update Patient Telecom information	Successfully update Patient's Telecom information
		Update Unknown Patient	Successfully update Unknown Patient
		Update Unknown Patient with Identifier	Successfully update Unknown Patient with Identifier
		Update Newborn Patients	Successfully update Newborn Patients

Table 12. Sample test scenario - eMPI

D. Terminology management portal

Test Case ID	Test Scenario Name	Test Scenario Description	Expected results
1.		Get Concept Map Translate operation	Translate from source code system to target code system

Table 13. Sample test scenarios – terminology management portal

E. Fast Healthcare Interoperability Resources (FHIR) APIs

Test Case ID	Test Scenario Name	Test Scenario Description	Expected results
1.	Create	Create {ProfileName} with Valid Data	Profile is expected to be created
		Create patient request should be directed to the EMPI	When the patient created in the clinical server is queried on the eMPI server, the result is expected to return created patient details
2.	Read	Read {ProfileName} for same HCP	{ProfileName} returned successfully
3.	Query	Searching {ProfileName} with search parameters	Successful Searching of {ProfileName} with search parameters
4.	Transaction Bundle	Send with Valid data at least 3 different entries	Successfully Sends Valid data for at least 3 different entries
5.	Update	Update {ProfileName} with Valid Data	Profile is expected to be updated
		Update patient request should be directed to the eMPI	When the patient updated in the clinical server is queried on the eMPI server, the updated result is expected to return.
6.	Operators	Metadata (Capability Statement)	Response has the capability statement of the clinical server

Table 14. Sample test scenarios – QHIE-Hub FHIR APIs

Healthcare providers should test scenarios below for all the QHIE-Hub FHIR profiles listed in **the target dataset & Interface specification provided as part of the onboarding resources.**

F. RHAPSODY - Health Level Seven API (HL7 v2) – where appropriate

Test Case ID	Test Scenario Name	Test Scenario Description	Expected results
1.	ADT (Admit, Discharge & Transfer)	Admit a Patient (ADT_A01)	Inpatient demographic record created for admitted patient
		Discharge a Patient (ADT_A03)	Patient is discharged/Encounter is closed
		Register a Patient (ADT_A04)	Register an Outpatient with demographic records
		Pre-Admit a Patient (ADT_A05)	Pre-Admitted Patient records should get created
		Update Patient Information (ADT_A08)	Patient information should get updated
		Cancel Patient Admit (ADT_ A11)	Patient admission is cancelled
		Cancel Patient Discharge (ADT_A13)	Patient discharge transaction is cancelled
		Merge Patient Information (ADT_A40)	Expected that 2 previously created patient records are merged
2.	Order	Lab Order (OML_O21)	Lab Order should get created/updated
		Imaging Order (OMI_O23)	Imaging Order should get created/updated/ cancelled
		Dietary Order (OMD_O03)	Dietary Order should get created/ updated/ cancelled
		General Order (OMG_O19)	General Order should get created/ updated/ cancelled
		Pharmacy/Treatment Administration (OMP_O09)	Pharmacy/Treatment Administration Order should get created/updated/cancelled
3.	ORU (Observation & Diagnostic Report)	Observation (ORU_R01)	Observation report should be created/updated
		Diagnostic Reports (ORU_R01)	Diagnostics report should be created/updated
4.	RAS and RDS (Pharmacy)	Pharmacy Order (RAS_O17)	Pharmacy order should be created/updated
		Pharmacy Dispense (RDS_O13)	Pharmacy dispense report should be created
5.	VXU (Immunization)	Vaccination (VXU_V04)	Vaccination records should get created/updated
6.	MDM (Documents)	Original document notification and content (MDM_T01)	Receipt of notification on creation of original document with content
		Document addendum notification (MDM_T05)	Receipt of notification of an addendum to the document without content
		Document addendum notification (MDM_T06)	Receipt of notification of an addendum to the document with content
		Document replacement notification (MDM_T09)	Receipt of notification of a replacement of the document without content
		Document replacement notification (MDM_T10)	Receipt of notification of a replacement of the document with content

Test Case ID	Test Scenario Name	Test Scenario Description	Expected results
7.	PPR(Problem)	Problem Add (PPR_PC1)	Problem information should get created
		Problem Update (PPR_PC2)	Problem information should get updated
		Problem Delete (PPR_PC3)	Problem information should get deleted

Table 15. Sample test scenarios – HL7 v2 APIs

If the facility is integrated to the platform using HL7 V2 specifications, then the below test cases should be executed by the healthcare provider to ensure successful connectivity and transformation.

G. eMeds FHIR APIs (Those are already executed part of FHIR)

Test Case ID	Test Scenario Name	Test Scenario Description	Expected results
1.	Create	Getting Doctor, Facility, Patient and Duration Unit information from the Core platform	Getting Doctor, Facility, Patient and Duration Unit information from the Core platform should get Created
		Getting Prescription Type, SIG code, Drug Descriptor and Route information from the Core platform	Getting Prescription Type, SIG code, Drug Descriptor and Route information from the Core platform should get Created
		Saving a prescription with prescription category	Saving a prescription with prescription category should get Created
		Saving a prescription with encounter class	Saving a prescription with encounter class should get Created
		Saving Prescription as Pending Signature	Saving Prescription as Pending Signature should get Created
		Successful Saving Draft Prescription	Successful Saving Draft Prescription should get Created
		Saving a prescription with maximum dosage of a drug	Saving a prescription with maximum dosage of a drug should get Created
		Saving prescriptions with drug interactions	Saving prescriptions with drug interactions should get Created
2.	Update	Updating Prescription as Signed	Prescription should get updated as Signed
3.	Cancel	Cancel a Signed Prescription	Signed Prescription should get Cancelled

Table 16. Sample test scenarios – eMeds FHIR APIs

H. eConnect (National clinical viewer) Embedded Viewer

Test Case ID	Test Scenario Name	Test Scenario Description	Expected results
1.	Get reference code	Get Concept Map Translate operation	Practitioner successfully gets Reference Code sent from EMR system which includes valid Facility ID, patient, and practitioner information for opening the eConnect Viewer as Embedded and ensure the right context is displayed (chosen facility, patient, and practitioner) is displayed
2.	Opening embedded viewer	On request, EMR will be opening the eConnect Viewer directly as Embedded with Valid Reference Code and Practitioner needs to log in while accessing first time in a day	Opening the eConnect Viewer as Embedded with Valid Reference Code and Practitioner logins seamlessly

Table 17. Sample test scenarios – eConnect

3. Conduct tests & generate reports

Healthcare providers are expected to start testing once all testing pre-requisites are satisfied, test data is ready, and scenarios have been developed. They must also get the credentials for the APIs, or the users for the solutions from MoPH. During testing, healthcare providers must ensure that all defects are captured. These need to be resolved and re-tested before connecting with the QHIE-Hub Prod environment.

Once tests are completed, healthcare providers must create an overall test report that captures the defects generated, their resolution status and any outstanding items (if any). A copy of these results may need to be shared with MoPH (particularly to inform the status of defects that were not resolved) for future review.

After performing the tests, HCPs must log all the defects in the recommended test report template. They must also share a report with MoPH when asked. The report should cover the date of resolution of those logged defects.

Test report Template

Test Case ID	Test Scenario Name	Test Scenario Description	Expected Results	Test Result	Tested Date	Tested By	Resolution Status	Date of resolution
1.	Embedd-ed Viewer	Opening the eConnect Viewer Solution as Embedded	Opening of the eConnect Viewer Solution as Embedded should be successful	<pass/ Fail>	<dd/mm/ yyyy>	<tester name>		

Table 18. Test report template

7.2 Onboarding Assessment

After completing all the exit criteria defined across the previous milestones, healthcare providers must fill in the Onboarding assessment to seek an "Onboarding clearance" to connect with the QHIE-Hub Prod environment. The Onboarding assessment will capture the completion status of the onboarding milestones as well as the pre-onboarding requirements as outlined in the roadmap. Healthcare providers must submit the completed checklist to their Facility manager.

A detailed template for the Onboarding assessment is shared with the onboarding handbook resources.

Based on the level of readiness and the current queue of onboarding, healthcare providers will be notified whether they have received onboarding clearance and their sequence. Once cleared, the facility manager will inform the healthcare providers about the earliest available start and end dates for the onboarding activities. Based on the size of the organization and volume of data, this period may span between a few days to weeks.

Onboarding assessment is used to track the readiness of a healthcare provider and their progress across the pre-defined milestones to determine the onboarding timelines. Once the onboarding clearance is received and the onboarding is scheduled, a healthcare provider will be informed about destination URLs to connect to Prod environment.

The facility manager will also inform the healthcare provider about the destination URLs to connect their production systems to the QHIE-Hub's Prod environment.

In case a healthcare provider has opted for data migration via CSVs, the link to the destination folder on Azure Explorer tool for data migration will also be shared by the facility manager.

*****


Mandate, policies &guidelines
Overview of national solutions
A. Get familiar with QHIE Hub
B. Get ready to onboard
Onboarding Roadmap
Implementation Plan
Change management
Meet requirements (security, integration, data)
Connect to sandbox to develop APIs
Map & transform data
Clean historical data
Validate patient demographics
Connect to Pre-prod to test workflows
Training
You are here
Complete onboarding assessment
Actual onboarding/production
Go live
GO LIVE
C. After you onboard
Drive adoption
Monitor data quality

CHAPTER 8

Onboarding steps

Once a healthcare providers receive a clearance from MoPH to proceed with onboarding, they are required to complete the below two steps as part of their actual onboarding and integration with the QHIE-Hub.

Figure 38. Steps to onboard

8.1 Connect to the QHIE-Hub Prod environment

A healthcare provider must follow the same steps outlined in Chapter 6.1.2 Network Connectivity to connect to the QHIE-Hub Prod environment using the GN Azure Hub or via ISP Hub. The destination URLs will be provided by the facility manager at the time of reviewing the Onboarding clearance checklist.

8.2 Execute historical data migration

This section outlines the steps required to migrate historical data from healthcare providers to the QHIE-Hub. It also outlines the duration of this data and additional rules that need to be followed. There are 3 stages to be followed as outlined in the figure *39*.

8.2.1 Prepare historical data according to QHIE-Hub requirements

All healthcare providers need to migrate data for the following target population.

- **Target population for data migration of Demographics (eMPI)**
  - All citizens of Qatar
  - All Residents with active and valid QIDs
  - All GCC-citizen visitors
  - For all other visitors only those who visited the Healthcare Facility in the last 2 years from the moment that Healthcare Facility is onboarded
- **Target population for data migration of health information**
  - Health data for Citizens of Qatar
  - Health data for Residents with active and valid QIDs
  - Health data for GCC-citizen visitors
  - No health data to be migrated for all other visitors
  - Health data for all patients included in the existing registries of healthcare provider organizations to Registries and care plans (eCare)

Given that the QHIE-Hub will not store historical scanned documents/images, healthcare providers who have paper records will need to digitalize their data at their own time/cost.

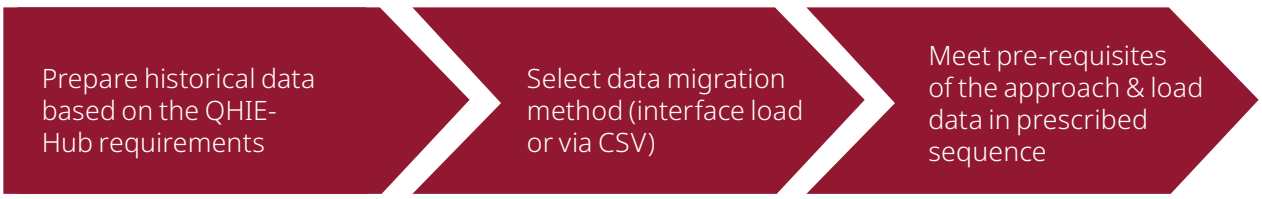


Figure 39. Sequence of activities for historical data migration

Type	Category	Dataset	Duration
Clinical	**Clinical data**	Vital signs	6 months
		Allergies & intoleances	Lifetime
		Problems& conditions (chronic)	Lifetime
		Problem & conditions (acute)	2 years
		Vaccine records	Lifetime
	Clinical documentation	Referral records	Active and pending
		Care plans	3 years
		Discharge summaries	10 years
		Clinical observartions/SOAP notes	6 months
	Conset	Consent & directives	Lifetime
	Diagnosis	Acute diagnoses	2 years
		Chronic diagnoses	Lifetime
		Diagnostic reports (includes radiology)	10 years
		Lab results	2 years
	Encounter details	Encounter information	2 years
	Medication information	Chronic medication	3years
		Acute medication	Active or latest records
	Patient history	Social determinants (e.g.. occupation, education)	Latest record
		Family history	Latest record
	Procedures	Performed procedures (i.e., diagnostic. interventional)	10 years
		Performed surgical procedures	Lifetime
Non-clinical	**Care team details**	Practitioner	Latest record
	Insurance & billing	Insurance information (non-claims data e.g., insurance type, policy number and insurer)	Latest record
	Order management	Service request	Pending requests
	Patient information	Patient information (i.e., name, QID, nationality, DOB, gender and address)	Latest record
		Related person	Latest record

Table 19. Duration of data for migration

Healthcare providers may seek exceptions as part of the onboarding review process through the facility manager. However, the final decision about the exception will reside with MoPH.

The duration of the data that healthcare providers need to migrate is shared in the table 19.

8.2.2 Select data migration method (interface load or via CSV)

There are two methods available for healthcare providers for data migration.

The first method is via API calls which is the strongly recommended method. This includes both FHIR R4B (national standard for healthcare data exchange) and HL7 v2.5.1 APIs (interim exchange standard supported by the QHIE-Hub).

The second method is via a CSV load which uses a standard set of predefined CSV templates shared by MoPH as part of onboarding resources.

All healthcare providers need to evaluate and select the applicable method.

- For migration through APIs, there are two steps:
    - **Transform:** Healthcare providers need to first transform data in sources systems for the required duration by implementing various business rules in the API gateway; these rules need to be tested in the developer environment where APIs are developed.
    - **Load:** After successfully completing the previous step, healthcare providers can send their data directly to the QHIE-Hub Prod environment using APIs
- For migration through CSVs, there are three steps:
    - **Extract:** Healthcare providers need to first extract historical data from source systems as per the data migration guide for the CSV template
    - **Transform:** Next step is for healthcare providers to transform this data by applying data coding standards, business rules etc.
    - **Load:** The transformed data needs to be uploaded first to the Pre-Prod environment (to assess quality), and then to the QHIE-Hub Prod environment in the prescribed formation to the shared location

Migration of historical data via CSV Loads should be an option of last resort that healthcare providers may use when they are unable to send their data through the interfaces in the first option.

8.2.3 Meet pre-requisites of the migration method & load data in prescribed sequence

a. FHIR R4B API standard method

In this method, healthcare providers are required to share data using the interface and technical specifications laid down by the QHIE-Hub. During FHIR R4B API calls, migrated data will go through the same validation rules as those for integration. Hence, in this method, healthcare providers must upload their historical data directly to the target system (Production environment) in accordance with the FHIR data model. Uploading historical data via this method is similar to real-time sync.

Pre-requisites that healthcare providers must meet before starting data migration through this method:

- Ensure that the healthcare provider messages are in sync with the QHIE-Hub Target Datasets and the required duration
- Ensure all business rules are applied in adherence to MoPH FHIR API specifications
- Ensure HCP system(s) are configured to send data in clinical bundles using FHIR R4B standard
- Ensure that the APIs are connected to Production Data Migration environment

Loading sequence: In this approach, healthcare providers must send all "Patient profile" data first. This should be followed by bundles of "Encounter" data (e.g., all encounter and encounter-related resources like observation, services request, procedure to be sent together for every encounter). Other profiles can be sent subsequently in bundles as per the loading sequence. All data must be sent in clinical bundles.

It is critical to follow the below mentioned loading sequence when uploading historical data. Since the profiles in the FHIR data model are related to each other, this structure must be preserved, and the below order must be followed:

1. **Root Resources:**
    a. Patient
    b. Encounter
2. **First Stage Resources:** Resources to be triggered with Patient
    a. FamilyMemberHistory
    b. RelatedPerson
3. **Second Stage Resources:** Resources to be triggered with Encounter
    a. AllergyIntolerance
    b. Appointment
    c. CarePlan
    d. CareTeam
    e. CommunicationRequest
    f. Condition
    g. DiagnosticReport
    h. DocumentReference
    i. Immunization
    j. MedicationRequest
    k. MedicationDispense
    l. MedicationAdministration
    m. MedicationStatement
    n. NutritionOrder
    o. Observation
    p. Procedure
    q. RiskAssessment
    r. ServiceRequest
4. **Third Stage Resources:** Resources to be triggered at the end
    a. EpisodeOfCare (imported with Condition, CareTeam and ServiceRequest
    b. Goal (imported with Condition and Observation)

The first-stage resources can be uploaded without the Encounter resource, but the Patient resource is a must for uploading. The second-stage resources cannot be uploaded without Encounter resource (e.g., if healthcare provider wants to upload CarePlan, they must upload both Patient and Encounter resources to the folder).

Resolving errors: Historical patient data should be sent to the target system as a bundle. In case there is an error(s) in the patient data, the bundle patient data will be rejected. Therefore, healthcare providers will need to re-send the patient data after fixing the error(s). A sample of the FHIR response with an error message generated in case there is an incorrect data record is given in Figure 40.

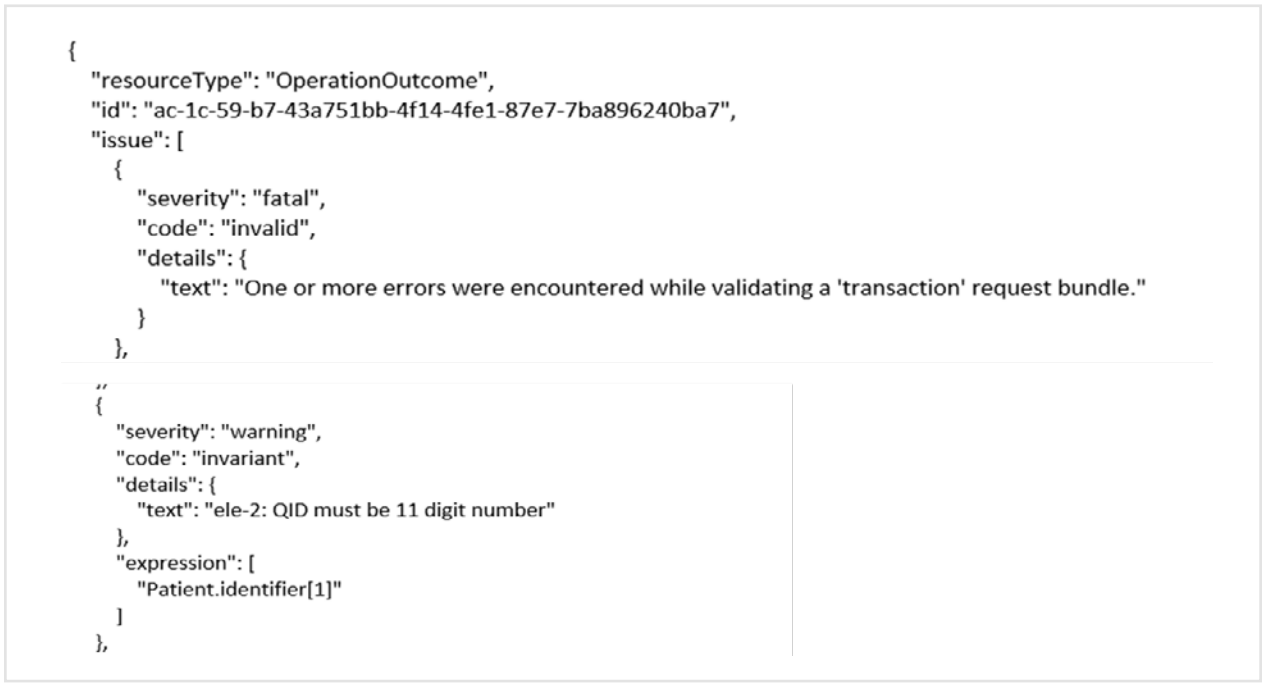


Figure 40. Sample error response for FHIR

b. HL7 V2.5.1 API standard method

In this method, healthcare providers need to send their historical data in the HL7 v2.5.1 format to the QHIE-Hub. The overall process will be similar to the one outlined above within FHIR.

Healthcare providers sending data through this standard need to conform with the HL7 v2.5.1 message format. It is important to note that there is no provision to accept messages of previous versions in this process. QHIE-Hub supports only the specified version of HL7 v2.5.1 messages. Clients that are using a different version should map message structures to the supported v2.5.1 message structure.

Healthcare providers will be provided with the definitions of HL7 v2.5.1 interfaces for Patient Administration, Order Management (including laboratory, radiology, dietary), Observation and Result Data Collection, Medication and Pharmacy Management, Medical records / information management.

Pre-requisites that healthcare providers must meet before starting data migration through FHIR:

- Ensure that the HL7 HCP messages are in sync with the QHIE-Hub Target Datasets and the required duration
- Ensure HCP system(s) are configured for HL7 V2.5.1 data exchange connectivity
- Ensure that the APIs are connected to Production Data Migration environment
- Ensure all business rules are applied and unit testing of the pipelines is done to ensure adherence to MoPH HL7 v2.5.1 specifications

Resolving errors: In case there is an incorrect data record, a N-ACK message is generated (sample Figure 41).

c. CSV load method

In this method, CSV files must be extracted, transformed, and loaded by the healthcare provider as per the shared data migration template that is mapped to the FHIR data specifications of the QHIE-Hub.

Pre-requisites that need to be met before starting data migration:

- Extract historical data based on the duration mentioned in the **Data migration CSV template** format provided as part of the onboarding handbook
- Ensure all patient demographics are updated as per the latest information for all historical data
- Apply data quality rules as per the **Data migration guide** provided with the onboarding handbook and ensure that the file is named as per specifications mentioned in the section below
- Load this extracted historical data from their source systems to the Data migration test environment for data quality check via the Microsoft Azure Explorer tool in batches (starting with a small batch of 10% of patients and progressively increasing the load to 30% and 60%)
- Resolve all data quality issues based on the error report
- Load the quality-controlled data to the QHIE-Hub Production environment via the same method using Microsoft Azure Explorer tool (in the same batch sizes)

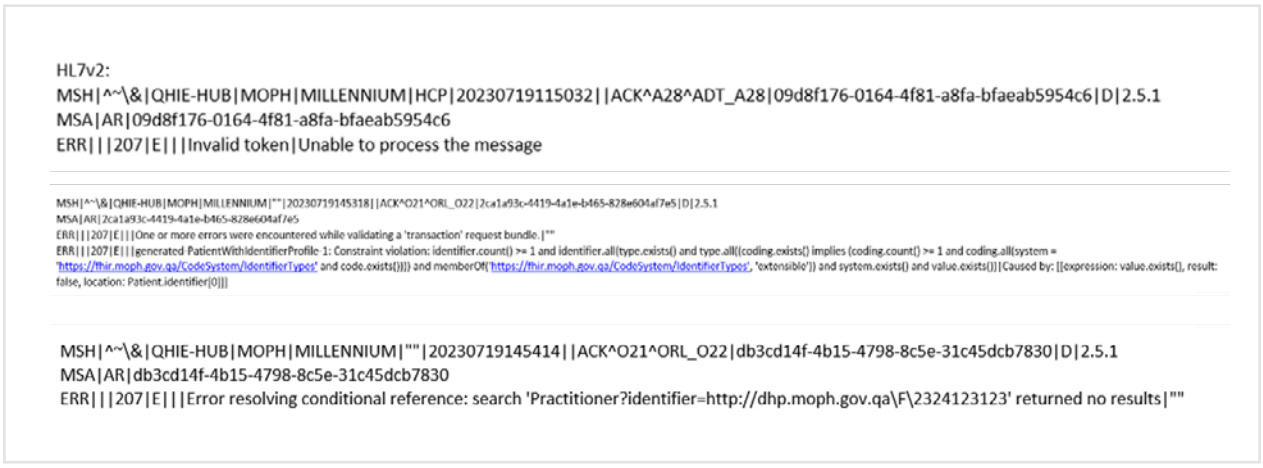


Figure 41. Sample error response for HL7

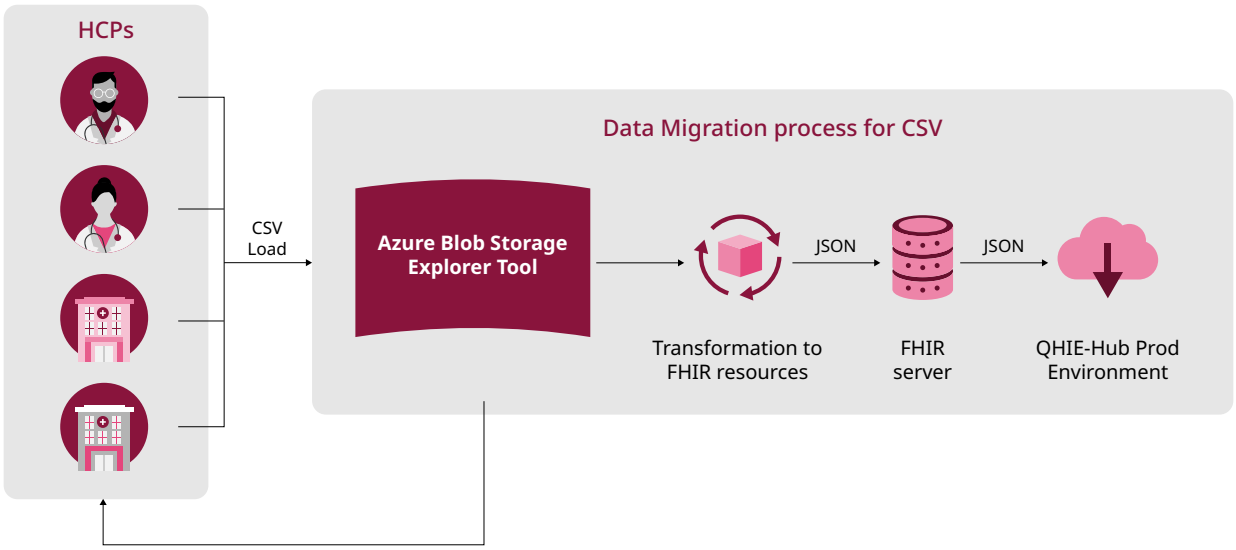


Figure 42. Conceptual diagram of data migration via CSVs

Only healthcare providers who meet the minimum threshold of the data quality (as determined from the results of loading the data in the data migration test environment) can transfer their data to the Production environment.

The following sub-section outlines how healthcare providers can use the tool to upload historical data into the Azure data migration test or production environments along with the naming convention to be followed.

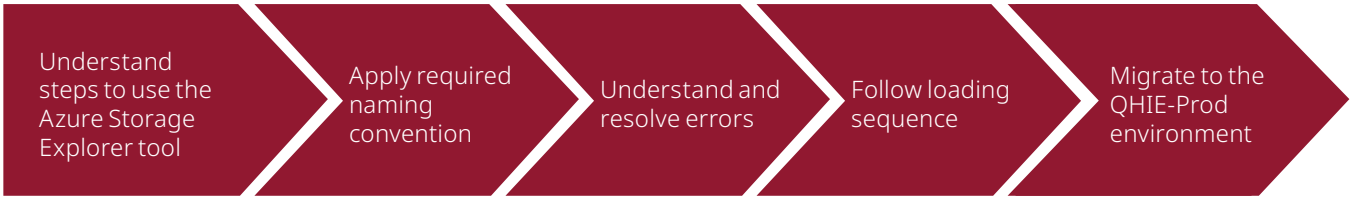
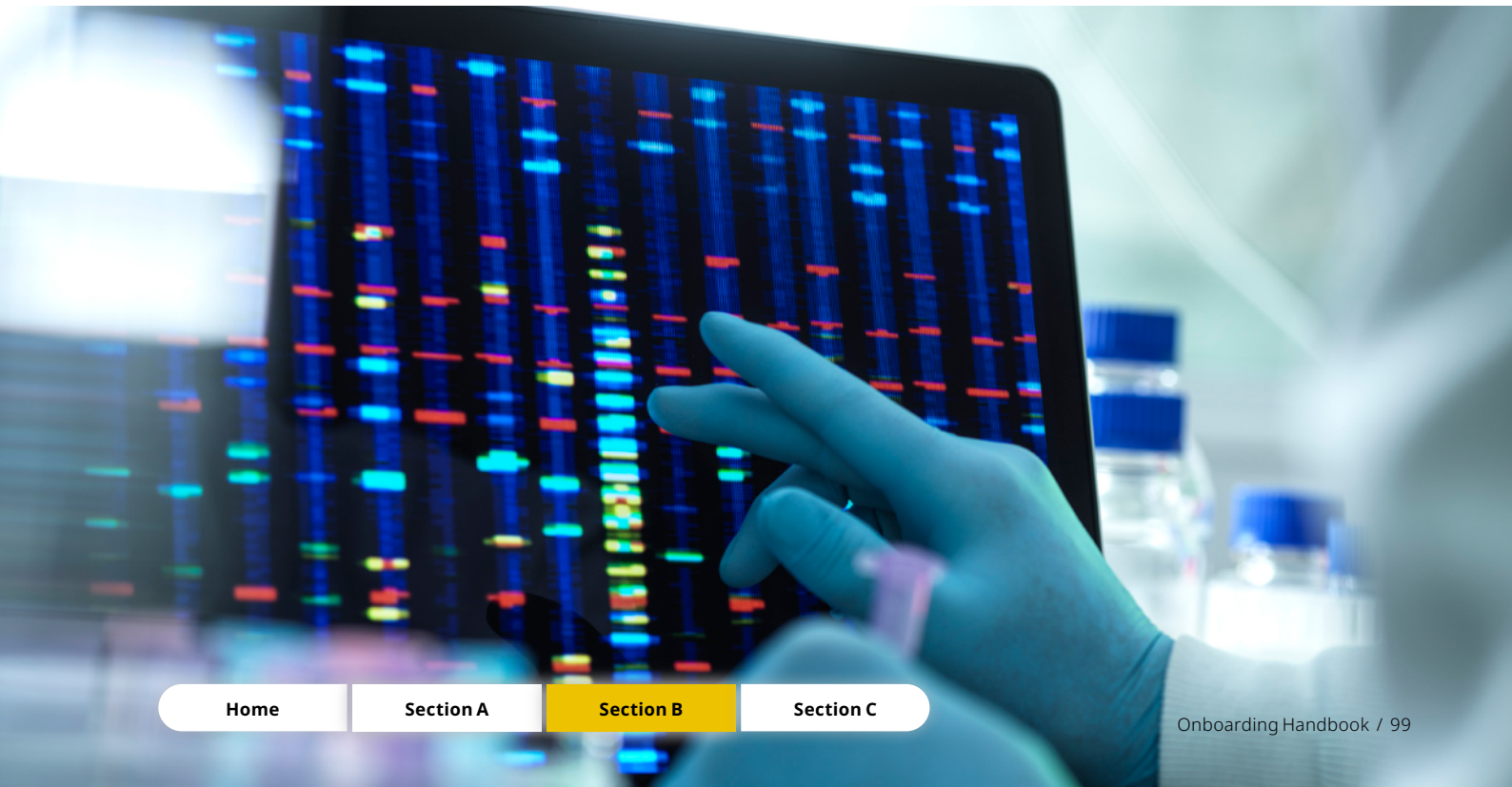


Figure 43. Using the Azure explorer tool for data migration



I. **Understand steps to use the Azure Storage Explorer tool to upload CSVs to the QHIE-Hub data migration or production environment**

The primary purpose of the Azure Storage Explorer tool is to provide a user-friendly interface for uploading and downloading files, creating and managing containers or folders and setting access permissions.

1

Download and install the Microsoft Azure Storage Explorer in the user's computer

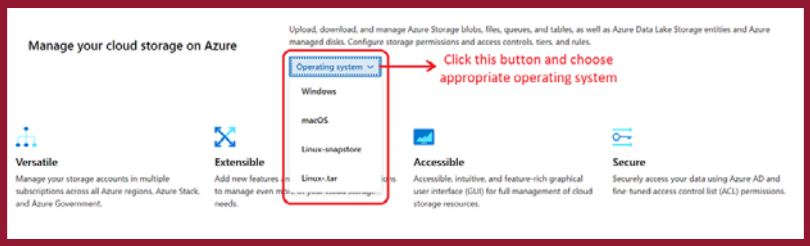


Figure 44. Choose the OS during download

a. Open a web browser on the user's computer and navigate to the official Microsoft Azure Storage Explorer website. (Click **https://azure.microsoft.com/en-us/products/storage/storage-explorer**)

b. Choose the appropriate download option for the user's operating system (Windows, macOS, or Linux).

c. Click on the download button to start the download process.

d. Once the download is complete, locate the downloaded installation file on the user's computer.

e. Double-click the installation file to launch the installation wizard.

f. Follow the on-screen instructions provided by the installation wizard.

g. Review the license terms and accept them if you agree with them.

h. Choose the destination folder where Azure Storage Explorer will be installed or accept the default location.

i. Select any additional installation options or components if prompted.

j. Start the installation process and wait for it to be completed.

k. Once the installation is finished, you may be prompted to launch Azure Storage Explorer to upload historical data.

2

Launch the Microsoft Azure Storage Explorer. Once launched, below is the screen that appears.

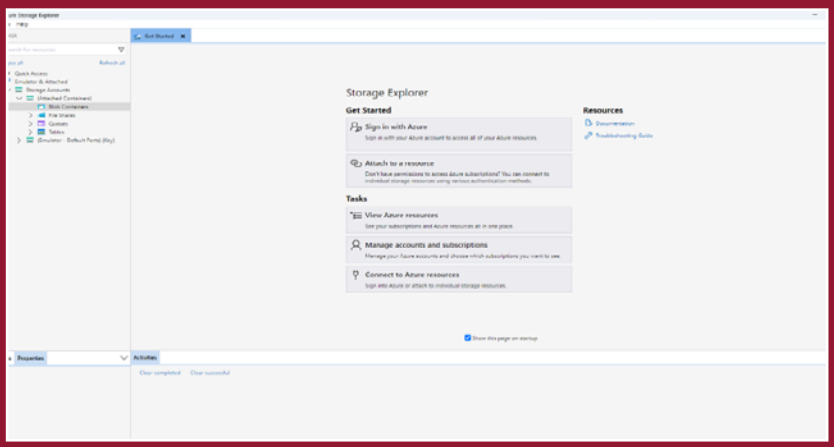


Figure 45. Azure Explorer landing screen

Microsoft Azure Storage Explorer provides various ways to access Azure Storage resources. **Healthcare providers need to use the Shared Access Signature (SAS) URL method. With shared access signatures, healthcare providers can upload their CSV templates securely with limited access to the environment.**

INPUT FOLDER SAS URL example:

https://stqhiepprdatamigqc001.blob.core.windows.net/migration/hcp1/input?st=2023-06-12T10:08:38Z&se=2023-12-12T18:08:38Z&si=Write&spr=https&sv=2022-11-02&sr=d&sig=AFYEY8DB7438v1hQBTMniQ61nVbj8oC6Kdy%2BJUbsl48%3D&sdd=2

OUTPUT FOLDER SAS URL example:

https://stqhiepprdatamigqc001.blob.core.windows.net/migration/hcp1/output?st=2023-06-12T10:09:13Z&se=2023-12-12T18:09:13Z&si=Read&spr=https&sv=2022-11-02&sr=d&sig=UiU8ESP%2BCQLYm32zdfD2srEu8D%2B73k9FGbyV2HUKXYc%3D&sdd=2

3 Access the Input Folder and Upload Files Steps

i Click Connect to Azure resources

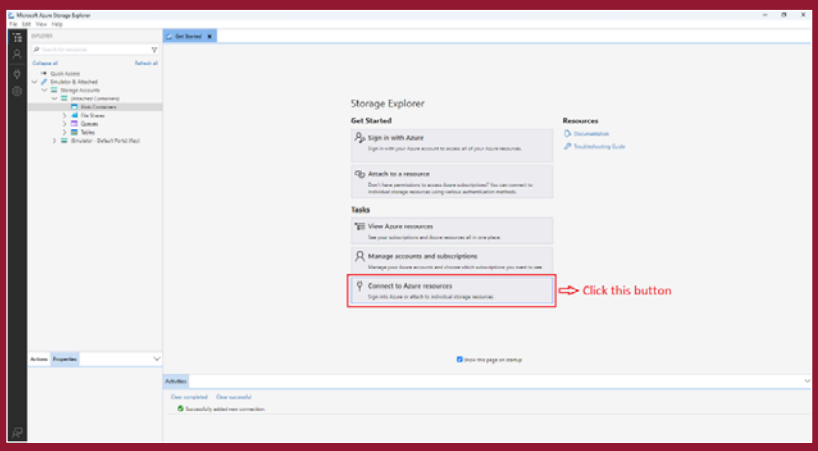


Figure 46. Connect to Azure resources

ii Click the ADSL Gen2 container or directory

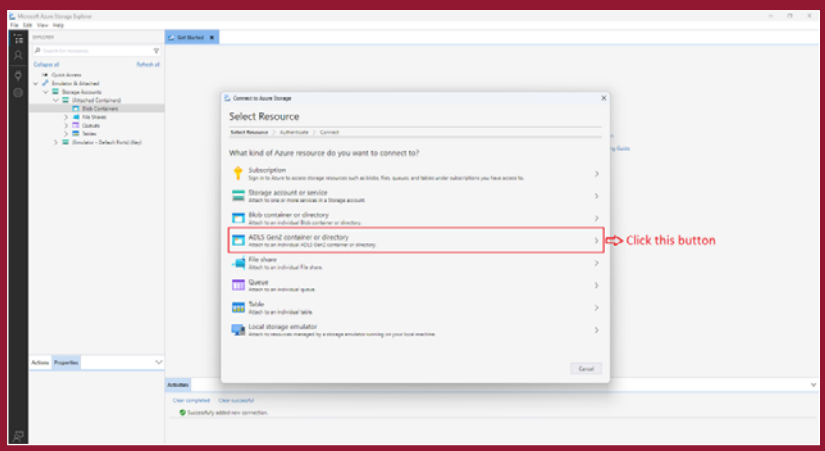


Figure 47. Choose ADSL Gen2 container or directory

iii Click the Shared Access Signature URL connection method and click next

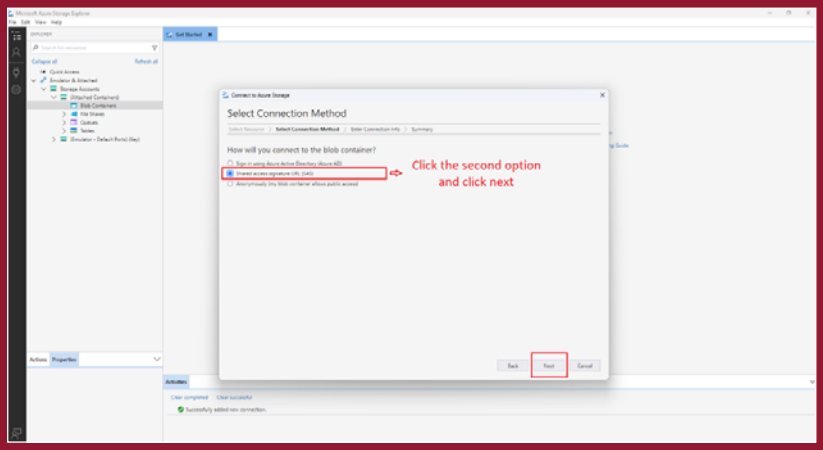


Figure 48. Choose SAS connection

iv Paste the SAS URL to access INPUT folder and click next. Enter the organization name in the "Display name" box. Paste the SAS URL that MoPH provided before.

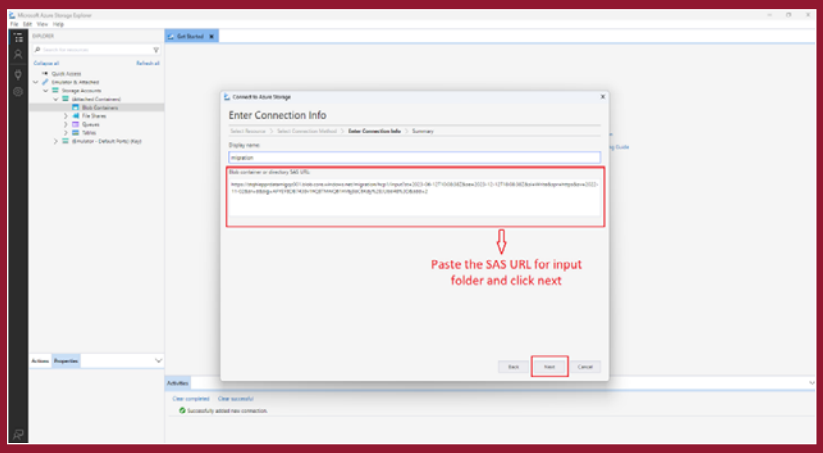


Figure 49. Paste SAS URL to INPUT folder

v Click the connect button to access the input folder. The summary of connection information can be seen here.

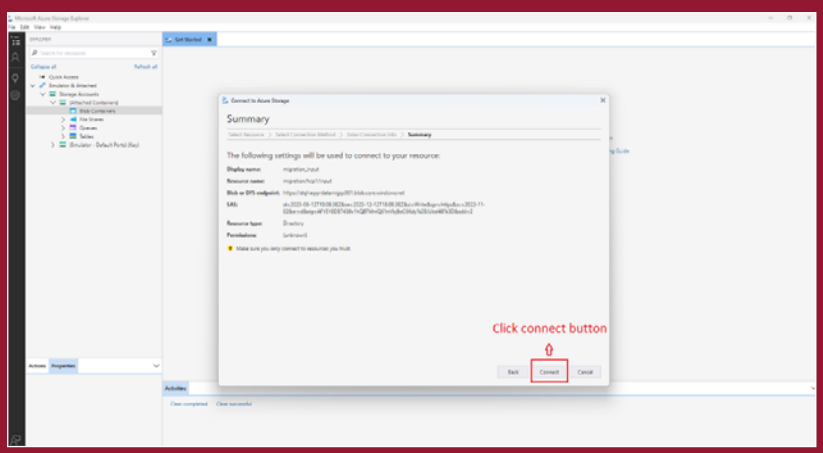


Figure 50. Access the INPUT folder

vi After "Successfully added new connection" is visible under the Activities, healthcare providers can upload their historical CSV data by clicking the "Upload" button and the "Selected files" button

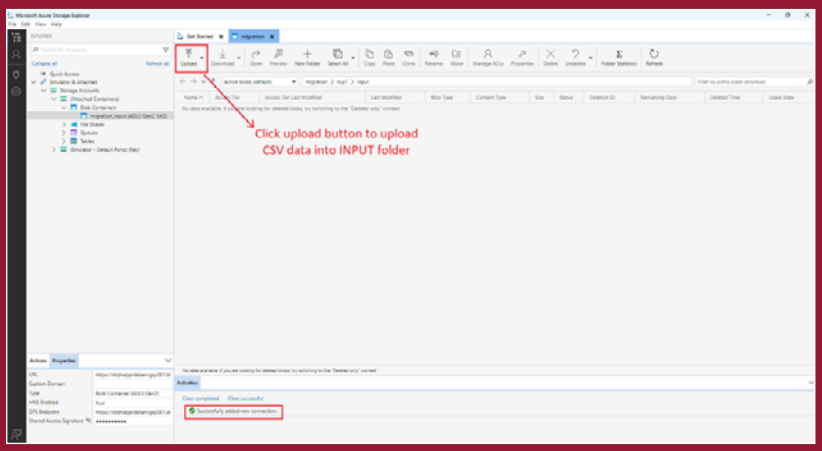


Figure 51. Upload CSV file

vii After selecting all files, press UPLOAD and click OK to successfully upload the CSV files to the Azure blob storage. In the activities box, the user will see a green tick message indicating that the upload process has been completed successfully.

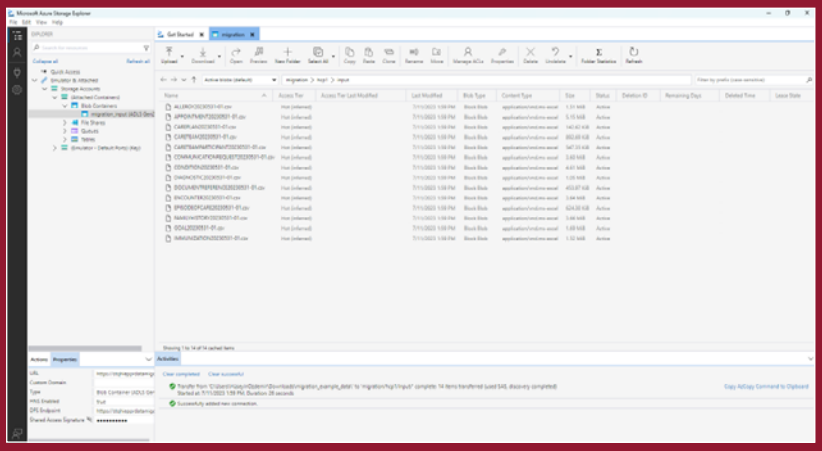


Figure 52. Confirmation of file upload

4 Access Output Folder and download the Reports

i As in the earlier step to access INPUT folder, healthcare providers can use the SAS URL given for OUTPUT folder to access it. Below are the steps to navigate to the OUTPUT folder. The remaining steps are the same as defined above.

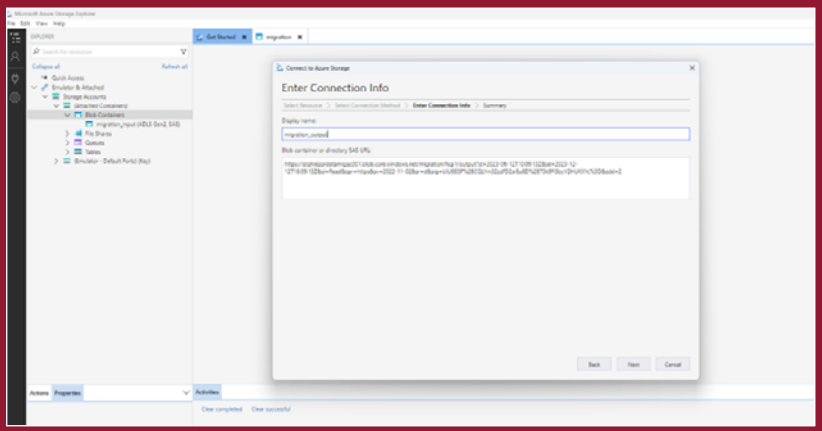


Figure 53. Access Output folder

ii After clicking NEXT, click the CONNECT button to complete the setup. Below is a screenshot of sample reports coming from the "CSV to FHIR JSON Converter"

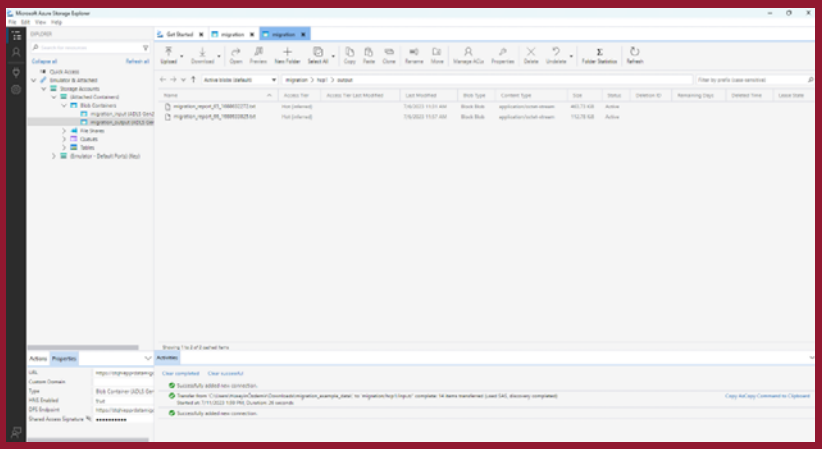


Figure 54. Sample output reports

iii Right-click any of the reports and select download.

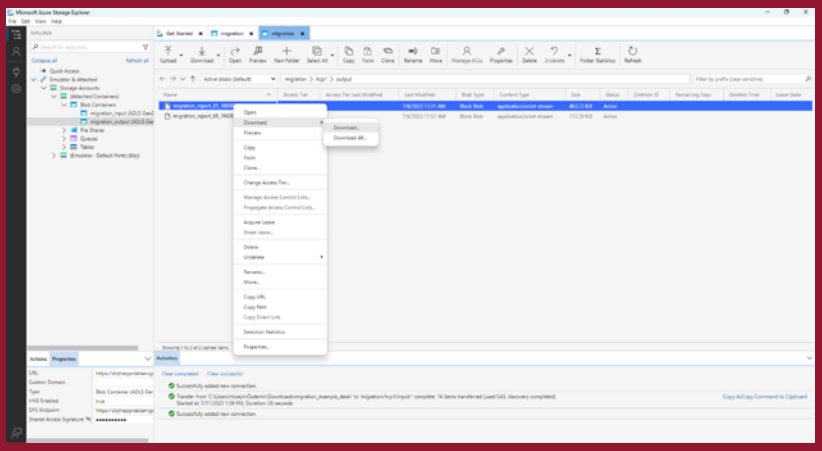


Figure 55. Download reports

iv After selecting the folder where the healthcare provider wants to download, the report(s) will be automatically downloaded. Healthcare providers can check in the Activities box the download status of these reports.

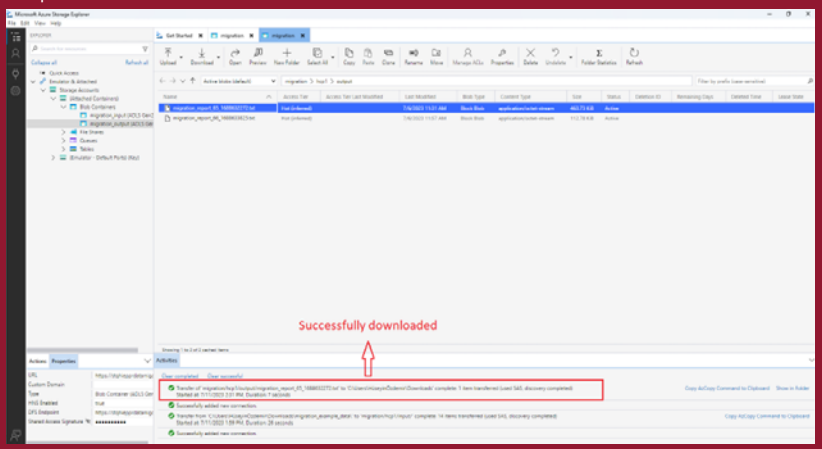


Figure 56. Confirmation of download

II. Apply required naming convention

Healthcare providers are required to follow certain naming conventions when uploading CSV files using the tool. **Files that are not compatible with this naming conventions will not be uploaded to the system and will not be analyzed.**

The name of CSV file must be **r'^ RESOURCENAME_\d{8}_.*\.csv$'**. This is a regular expression that describes a specific pattern for filenames in CSV (Comma Separated Values) format.

- **r:** This denotes a raw string literal in Python, meaning that escape sequences (e.g., **\n, \t**) are not processed, and the string is used as-is. This is commonly used with regular expressions to avoid conflicts with backslashes.
- **^**: This anchor symbol asserts the start of the string. It ensures that the pattern must start matching from the beginning of the input string.
- **RESOURCENAME_**: This part of the pattern is simply a literal string that must match exactly as it is. The mentioned "RESOURCENAME" refers to FHIR resources like patient, encounter, allergy, etc. So, if a specific FHIR resource names needs to be matched, "RESOURCENAME" needs to be replaced with the desired resource name (e.g., "patient", "encounter", "allergy").
- **_\d{8}_**: Here, the underscore _ matches the character "_" literally. \d{8} is a quantifier that matches exactly eight digits. This pattern is used to match a date in the format "YYYYMMDD". For example, "20230717" is a valid match.
- **.***: This part of the pattern matches any character (except for a newline) zero or more times. It allows for any additional characters to appear after the date in the filename. Healthcare providers are expected to write their entity name after the date.
- **\.csv**: The dot . is a special character in regular expressions that matches any character. To match a literal dot (.), you need to escape it with a backslash \.. So, \. matches the dot character literally. **csv** matches the string "csv" exactly.
- **$**: This anchor symbol asserts the end of the string. It ensures that the pattern must continue matching until the end of the input string.

The table 20. shows sample CSV names for all resources that HCP1 plans to upload on 13 July 2023.

EXAMPLE NAMING CONVENTIONS
ALLERGY_20230713_HCP1_00.CSV
APPOINTMENT_20230713_HCP1.CSV
CAREPLAN_20230713_HCP1.CSV
CARETEAM_20230713_HCP1.CSV
CARETEAMPARTICIPANT_20230713_HCP1.CSV
COMMUNICATIONREQUEST_20230713_HCP1.CSV
CONDITION_20230713_HCP1.CSV
DIAGNOSTIC_20230713_HCP1.CSV
DOCUMENTREFERENCE_20230713_HCP1.CSV
ENCOUNTER_20230713_HCP1.CSV
EPISODEOFCARE_20230713_HCP1.CSV
FAMILYHISTORY_20230713_HCP1.CSV
GOAL_20230713_HCP1.CSV

EXAMPLE NAMING CONVENTIONS
IMMUNIZATION_20230713_HCP1.CSV
MEDICATIONADMINISTRATION_20230713_HCP1.CSV
MEDICATIONDISPENSE_20230714
MEDICATIONSTATEMENT_20230713_HCP1.CSV
MEDICATIONREQUEST_20230715
NUTRITION_20230713_HCP1.CSV
OBSERVATION_20230713_HCP1.CSV
PATIENT_20230713_HCP1.CSV
PROCEDURE_20230713_HCP1.CSV
RELATEDPERSON_20230713_HCP1.CSV
RISKASSESSMENT_20230713_HCP1.CSV
SERVICEREQUEST_20230713_HCP1.CSV

Table 20. Sample CSV file names for 13th July 2023

Below are few examples of filenames that will NOT match this pattern:

- Incorrect resource name:
  - File: encounter_20230717_HCP1.csv
  - Explanation: The resource name should match the pattern RESOURCENAME, but here, "encounter" is used in small case.
- Missing underscore after date:
  - File: patient_20230717HCP1.csv
  - Explanation: There should be an underscore after the date, but it is missing in this example.
- Missing ".csv" extension:
  - File: patient_20230717_HCP1
  - Explanation: The filename should end with the extension ".csv", but here, it is missing.
- Extra characters after ".csv":
  - File: patient_20230717_ HCP1.csv_backup

Explanation: The filename should end with the extension ".csv", but here, it has additional characters after ".csv".

III. Follow the Loading Sequence

Healthcare providers are required to prepare all CSV files and upload them together (as a bundle). Failure to do the above will break linkages in the FHIR data model across the profiles, leading to failure in uploading the files and generating the report.

The only exception to the above rules is during the validation of patient demographics where only "Patient" resource data needs to be uploaded.

Healthcare providers must upload their historical data beginning with the most recent records and progressively move backward in time to older data. This methodology ensures:

- Most up-to-date information is promptly available in the new system, facilitating real-time access to the latest patient data
- Reduces the risk of delays in processing critical and current patient information
- Allows healthcare providers to focus on resolving any potential data inconsistencies or issues that may be more prevalent in recent records, as they are more frequently accessed and updated
- Enables providers to gain an immediate understanding of the current state of their patient data, aiding in the efficient clinical management and decision-making processes.

IV. Understand & resolve errors

After the first cycle of uploading the CSV file to the Data Migration Test environment, healthcare providers may encounter two types of errors.

- Errors caused by the user: This includes certain errors identified in the system caused by user input. Users are requested to fix these errors and submit the necessary corrections to ensure that their requests are processed accurately.
- Errors caused by the system: This includes errors that are system-generated and do not require any action from the user. These errors will be fixed automatically.
- Messages related to these errors are listed in the **table 21.**

Some other examples of error codes that are mentioned below:

- Converter errors:
    a. The converter failed due to a logic problem. *(e.g., wrong type for a choice type field)*
    b. The converter did not find a mandatory field. *(e.g., missing id)*
    c. The converter received a field that was not the expected type. *(e.g., birthdate is Boolean)*
    d. The value of a field did not make sense when converted. *(e.g., negative age)*
    e. The data does not conform to FHIR. *(e.g., uses a non-existent enum value)*
- Profile errors:
    a. The data does not conform to the specified profile as defined on the FHIR server.
    b. The FHIR Profile has a logical error in the definition. *(e.g., asks for an impossible state)*
    c. The FHIR Profile does not conform to the Target Data Set. *(e.g., mandates optional data)*
- Reference errors:
    a. A resource tried to reference a non-existent reference.
    b. A resource tried to use Conditional Referencing, but the query failed.

	User error message templates	Examples
Errors caused by the user	**"UNDEFINED_FILE_TYPE"**:"00001-File name and/or type does not match the format",	00001-File name and/or type does not match the format: Filename: _CAREPLAN20230710-01.txt Expected Filename format: <RESOURCE_NAME>_<YYYYMMDD>.csv
	"ROW_COUNT_MISMATCH":"00002-Number of rows are not equal to the defined in the header-> ",	00002-Number of rows are not equal to the defined in the header-> Resource: NUTRITIONORDER, Header:56467, NumOfRows:56468
	"COLUMN_COUNT_MISMATCH":"00003-Column count is not compatible with header->",	00003-Column count is not compatible with header-> Resource:appointment, Expected Column Count:32, Non-Matching Line Number (Count of columns): 1(31),2(31),3(31),4(31),5(31),6(31),7(31), ...
	"COLUMN_MISMATCH":"00004-Name of columns in the header do not match the columns defined for the Resource:	00004-Name of columns in the header do not match the columns defined for the Resource:appointment, Expected Column Count: 32, Header Column Count: 31
Errors caused by the system	**"SYSTEM_ERROR"**:"00100-The system cannot process the file(s) properly. User intervention is not required as the errors will be fixed automatically."	00100-The system cannot process the file(s) properly. User intervention is not required as the errors will be fixed automatically.

Table 21. Sample error nessage

c. A resource used Temporary Referencing, but it did not exist in the bundle.

- Data errors:
  a. The data does not conform to the FHIR.
  b. Two mutually exclusive fields are set.
  c. *the combination of two fields violates the FHIR specification*

V. Migrate to the QHIE-Hub Prod environment

Healthcare providers are required to repeat the above process of uploading and resolving data quality issues in the Data migration test environment across multiple cycles until they reach full compliance with prescribed rules. Only once this milestone is achieved can they proceed further.

Healthcare providers will receive the Input SAS URLs for the QHIE-Hub Prod environment after MoPH has reviewed their onboarding assessment results and has provided an Onboarding clearance.

Healthcare providers are required to follow the steps outlined in this section to subsequently upload this data to the QHIE-Hub Prod environment. With this approach, there should be no data errors in this stage.

Data migration will be deemed completed when all files have been uploaded successfully.

8.3 Training

As a part of the onboarding process, MoPH will conduct training on the QHIE-Hub solutions for all the relevant healthcare provider stakeholders (including both practitioner and non-practitioner staff) in a "Train-the-trainer" format. This chapter covers the key training objectives, and the list of activities healthcare providers must complete to ensure all end-users are trained on the QHIE-Hub solutions by leveraging the resources provided by MoPH.

The overall sequence of activities is outlined in the figure 57.

8.3.1 QHIE-Hub training objectives

The Table 22. provides an overview of learning objectives for each of the QHIE-Hub solutions as well as the competencies to be instilled in the trainees when they complete the respective training modules. These determine the agenda and the content for the training modules developed by MoPH.

MoPH will train the relevant stakeholders nominated by each healthcare provider in a train-the-trainer format for a smooth onboarding purpose who will then train the end-users of the solution.

8.3.2 Training phases

When a healthcare provider's readiness for onboarding is established, MoPH will extend an invitation to initiate and plan trainings starting with nominated trainers, followed by end-users of an organization. Below is a high-level overview of activities healthcare providers must undertake before, during and after the training phases.

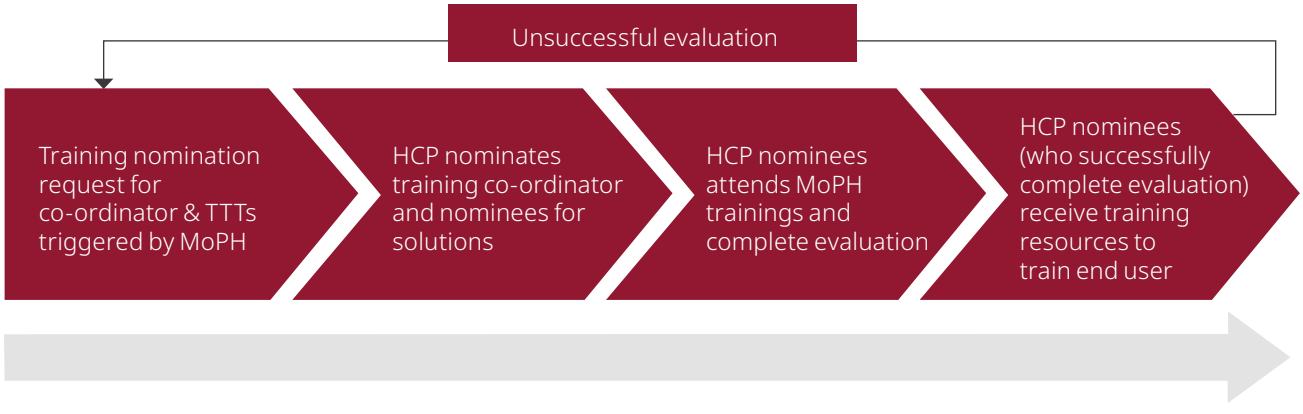


Figure 57. Sequence of activities in training

Solution	Learning objectives	Competencies to be instilled
QHIE-Hub Platform (Only for Super Users/ designated QHIE-Hub platform admins)	Learning how to manage, operate and maintain the different services under the QHIE-Hub Platform such as FHIR, terminology	**EMPI** • Understand how to integrate with EMPI and its benefits • Recognize the technical requirements for the healthcare provider • Identify the business workflows and administration requirements for the healthcare provider **Healthcare provider Identity Management portal** • Be able to navigate the overall portal • Understand how to add/remove and modify users such as practitioners **Terminology** • Know the new data terminology's standards and identify its use • Understand how to navigate the portal to download and use mandatory code sets, concept maps etc.
eConnect (National clinical viewer) (for all practitioner staff)	Learning how to navigate and access patient data for the purposes of clinical decision making and reconciliation.	• Identify the different types of data to be displayed in a patient summary if consent is provided (e.g., ongoing diseases, allergies, medication, care plans, vaccinations, surgeries) • Distinguish the patient information access level for each stakeholder (e.g., physicians' access level, insurance company level) • Know the patient emergency access level and usage (e.g., how physicians can access a patient's health records without approval in an emergency) • Navigate the monitoring and tracking mechanism of patient data (e.g., viewing the audit log)
eMeds (e-Prescription and Digital Pharmacy) (all pharmacists and practitioner staff)	Learning how to electronically prescribe and manage prescriptions. Learning how to electronically dispense medication and manage prescriptions	• Use the ePrescription and Digital Pharmacy (eMeds) system (e.g., details about all the modules) • As a pharmacist, understand how to access and dispense a prescription • As a practitioner, understand how to prescribe medicines to patients • Control substance prescriptions through notifications based on patient data • Manage (stop, pause, reduce) prescriptions based on data history
eCare (Registries and care plans)	Learning how to add patients to registries and create care plans Learning how to use reports and statistics generated from disease and condition registries Learning how to manage elements of care plans	• Use the eCare (Registries and care plans) system (e.g., details about all the modules) • Add patients to and remove patients from registries • Create care plans based on guideline recommendations • Create care teams for patients and send messages to care team members and patients • View reports and statistics generated form the registry data • View registries of patients with relevant information • As a eCare Definitions Admin, understand how to manage diseases, disease pages, questionnaires, clinical concepts, and educational materials

Table 22. Training objectives

Figure 58. Overview of activities across training phases

8.3.3 Pre-training phase

1. **Take note of training schedule and nomination form**

   MoPH will define a training schedule based on the training objectives across solutions, topics, medium and target audience. The training schedule will be shared with the healthcare providers along with the training nomination form. All healthcare providers who are invited to be onboarded by MoPH will be provided with the training nomination form and along with details about the expected number of trainees, learner personas and training profiles. Healthcare providers are expected to take note of the schedule and the details required in the nomination form.

2. **Nominate a training coordinator**

   To successfully co-ordinate trainings with MoPH and leverage all materials available, healthcare providers must identify a training coordinator and share his/her contact details with the MoPH. The training coordinator will be the **only point of contact** between healthcare provider and MoPH for all training-related activities.

   Key responsibilities of the training coordinator

   a. When the MoPH sends a letter requesting for nominees to attend the training sessions, the training coordinator should identify profiles that match the requirements in the nomination letter and reply (via email or through the link provided by MoPH) to the MoPH in a timely manner.

   b. The training coordinator is expected to ensure that the nominee(s) can attend the training sessions and are excused from all work-related obligations during the training (with the exception of emergencies).

   c. In case a nominee can no longer attend the training, it is the training coordinator's responsibility to ensure that this is communicated to the MoPH. Failure to communicate this will result in a 'no show' from your entity and failure of the training for that respective nominee.

   d. The training coordinator is expected to ensure that all training related communication from QHIE-Hub is shared with the respective stakeholders (i.e., nominee requirement, training details, etc.)

3. **Nominate trainees based on learner persona/profiles**

   For every solution, healthcare providers must nominate trainees based on the learner personas (Train-the-trainer or Super user), trainer characteristics, and other considerations.

   There are two main learner personas for whom training has been planned.

a. **Train the Trainer**

- Train the trainer profile covers stakeholders who will participate in the training and, in turn, give the training within their respective organizations.
- Train the trainer can be an existing or nominated person. These trainers need to know the healthcare domain and ideally be familiar with Healthcare Informatics.

b. **Super User**

- Super user profile covers stakeholders who should be familiar with the system and application configuration.
- They can be system administrators who can manage and configure system functionalities. They should have knowledge and experience in IT and health informatics.

The table 23. shares an illustrative trainee persona with details about their learning profile, skill-set and prior experience who will receive the solution training.

Training nominees will receive a registration email and are required to fill out their details (when applicable). They will receive all log-in details (when applicable) one week before the training session along with all training-related details. Training nominees must follow the instructions received in their log-in email to access the training material/environment. They can reach out to their organization training coordinator in case they face any difficulties and request support from MoPH.

If a healthcare provider organization does not have trainers or individuals who can play the role of a trainer, the training coordinator must inform MoPH to request for alternative solutions (such as access to self-learning materials, online trainings for end-users etc.).

4. **Gain access to training materials and resources**

MoPH will use different training media based on the training requirements. These include:

- **Classroom training** – a traditional format where trainees can gather at a physical location to learn from MoPH instructors/ subject-matter experts about the onboarding steps, features of the national solutions, new business workflows, along with how to use the solutions on a day-to-day basis.
- **Virtual live training** – where trainees can participate in the training virtually from a remote location (instead of a traditional classroom or designated training environment). The training will be conducted via videoconferencing/ collaboration tool, and these sessions will be recorded and shared in a centralized learning platform created by MoPH.
- **eLearning or self-paced training** – where the learners are in control of the pace of their learning. It allows trainees to continue learning and developing skills at their own pace with additional resources.

These trainings will be carried out in both English and Arabic. Training coordinators must enroll participants in the sessions based on their respective language preferences.

Personas	Learning Profile	Skill Set Required	Experience
Clinical Trainers	Train the Trainer	• Basic computer literacy • Training skills • Experience in EMR applications • Healthcare applications and systems knowledge are preferred • Clinical code set and medical literacy/ terminology are preferred	5 years

Table 23. Illustrative training personas

Self-Paced training materials of all relevant solutions, including training manuals, recorded training videos, and supplementary documents, will be centrally stored and be accessible by the trainees via the QHIE-Hub Training web page.

MoPH will also prepare learning resources for all QHIE-Hub solutions that will be shared with all the trainees. These include:

- **End-user manuals:** These manuals explain how the system can be used by the end users, and features/functionalities available. These are based on the final design of each of the solutions.
- **Train the Trainer Training Materials:** Trained instructors/trainers will use these for the End User and Super User training sessions of each Solution. Training materials will have content specific to the intended learner profile and will be in different formats such as image, video, text files.
- **Training Guide:** This implementation guide provides an overview of different training approaches that can help healthcare providers plan trainings for end-users to use and adopt the QHIE-Hub solutions.
- **E-learning videos:** This includes a set of pre-recorded training videos or recorded meetings in a modularized format for different topics in each solution.

5. Understand training topics for end-users

Training topics are designed based on the outcomes of the training needs assessment. Solution topics are detailed for different features of every solution. Healthcare providers are expected to take note of these topics, their medium, duration etc. and inform their nominees/end-users about the time-commitment required from them.

6. Gain access to training environment.

MoPH will enable QHIE-Hub solution training in an earmarked training environment. All solution modules with the complete list of features, identical to the actual live solution will be made available and accessible on the training environment

The training environment will have sample patient data, which will be created according to the training scenarios. All nominated trainees have access to the training environment before the training session.

Training user accounts will be created for each trainee in the training environment one week before the training. These accounts will only be used during training and authorized according to the training scope. User access to the training environment will be valid only for the nominated training session.

Training Area		Topics	Medium	Practice required on Screen	Duration
User Information	User Operations	On-screen explanation of the login mechanism and the authentication rules	Virtual-live Training	Not Required	30 minutes
		On-screen explanation of how to search patient information			
		On-screen explanation of the Patient Profile Information	Virtual-live training	Not Required	30 minutes
		On-screen explanation of the Quick Access Menu & Patient Change and other functional buttons	Virtual-live training	Not Required	30 minutes

Table 24. Illustrative Health Information Exchange training topics

8.3.4 During Training

1. Attend training

Training may be scheduled virtually or in-person. The type of training and location will be provided for the attendees in the training invite. During the training, trainees must attend the sessions on time and must complete all training requirements (i.e., evaluation, feedback).

Every training session will have the following:

- Walkthrough of the content tailored to the respective module,
- On-screen practice (when applicable)
- Guidance on how to train other end users

As part of standard training practice, attendance will be taken by the trainer for each lesson at the end of each session. A follow up communication with no-shows will be done within 24 hours after the class.

2. Complete evaluation

At the end of a training, an evaluation in the form of an online quiz about the topics covered will be conducted. This quiz will have a set pass percentage. All trainees are expected to achieve the minimum pass marks for a successful evaluation. Outcomes of training evaluation:

- Upon successful evaluation, trainees will be given a training certificate
- In case of an unsuccessful training outcome, the trainee will be provided with another opportunity to attend the training.
- User access will only be enabled to the QHIE-Hub solution only trainees have cleared their evaluation.
- Trainees must complete the evaluation related to the training they received and must pass the evaluation to be able to mark the session as completed.
- Based on feedback from trainees, and if the evaluation at the end of a session is unsatisfactory, re-training will be considered

3. Provide training feedback

At the end of the training session, all trainees will be asked to fill out a feedback form. This includes providing comments and assessing the quality of the content. Trainees are requested to fill the form to provide their feedback on how to improve the program's learning content and instructional methods.

8.3.5 Post training activities

1. Plan and conduct internal trainings within the organization

After trainers have received training from MoPH, they should work with the training coordinator to carry out the end-user trainings in their respective facilities. The training coordinator must ensure that trainers have the resources needed (i.e., location, set up etc.) and end-users participate. These trainings should be conducted in line with the training manuals (to be made available by MoPH to healthcare provider trainees).

Even after onboarding, trainers need to continue providing end-user training, particularly to new users. Eventually, these trainers are expected to become champions/ change agents who will continue to drive adoption of the QHIE-Hub national solutions within their facilities.

2. Report end-user training and assessment status

After every internal, end-user training, trainers are expected to administer an evaluation to the attendees in the form of an online quiz. This can be designed using the end-user training manuals. All end users must be trained and must pass the evaluation before getting access to the QHIE-Hub solutions. If an end-user is unsuccessful in clearing the evaluation, re-assessment or re-training must be provided to them by the training coordinator. Healthcare providers must keep a record of the pass/fail status along with individual transcripts of the online assessment for every trainee for future reference.

As part of go-live and bulk-user creation, the training coordinator must report the training status of the end-users to the facility manager. User accounts will be created only when the facility manager has confirmed that end-user training and assessment has been completed for all users.


Mandate, policies &guidelines
Overview of national solutions
A. Get familiar with QHIE Hub
B. Get ready to onboard
Onboarding Roadmap
Implementation Plan
Change management
Meet requirements (security, integration, data)
Connect to sandbox to develop APIs
Map & transform data
Clean historical data
Validate patient demographics
Connect to Pre-prod to test workflows
Training
Complete onboarding assessment
You are here
Actual onboarding/production
Go live
C. After you onboard
Drive adoption
Monitor data quality

8.4 Go-Live

The go-live phase starts after a healthcare provider has successfully integrated their production environment with the QHIE-Prod environment and has migrated all the historical data. It must be initiated within the onboarding window provided to the healthcare provider by the facility manager. During this period, MoPH will bulk-upload and create accounts for all trained end-users shared by the healthcare provider. Once completed, the facility manager will provide confirmation to the healthcare provider so that end-users may be notified and can login.

It has two steps as shown below.

Figure 59. Steps to be completed in Go-live phase

8.4.1 Bulk registration of end-user accounts

This section outlines the steps that healthcare providers need to follow to create users and enable their access to the national solutions part of the QHIE-Hub.

Each healthcare provider will be responsible for ensuring that its domain name is registered, its users requesting access have a valid corporate email id and have passed the internal training assessment.

The QHIE-Hub uses **Azure Active Directory B2C** to create and authenticate healthcare practitioners as well as non-practitioner staff across its national solutions (including QHIE-Hub Platform, ePrescription & Digital Pharmacy & eConnect). **It is important to note that onboarding of healthcare provider users requires a valid and active corporate email id from a registered domain.** Each healthcare provider will be responsible for ensuring that its domain name is registered, its users requesting access have a valid corporate email id and have passed the internal training assessment.

Furthermore, since Health Information Exchange & ePrescription and digital pharmacy (eMeds) , and Registries and care plans (eCare) need to be accessed only by healthcare practitioners, credentials of the practitioner will be verified against databases from Department of Healthcare Professionals (DHP), MoPH's licensing department. Therefore, healthcare practitioners need to ensure that their information (including mobile phone number) is always up to date in MoPH's records and is the same as the information available with their respective organizations.

To create local accounts for their users in the QHIE-Hub's Azure Active Directory B2C, healthcare providers need to share details about their users during onboarding for bulk user creation by MoPH. Subsequently, they can manage the list of users via the self-service capabilities of the healthcare provider Identity Admin portal. The Figure 61. describes the onboarding and authentication flow for healthcare provider users (both Practitioners and Non-Practitioners).

During onboarding, healthcare providers are required to share details of all their staff (both practitioners and non-practitioners) along with other attributes for bulk user creation. These attributes include:

- Full Name (Per ID)
- Email ID (**Only Corporate Email ID**)
- Health Care Provider Name
- Corp ID No.
- License Number (applicable for licensed Practitioners)
- ID Type (e.g., QID, Passport)
- ID Number
- Mobile Number (**Must match the one in DHP**)

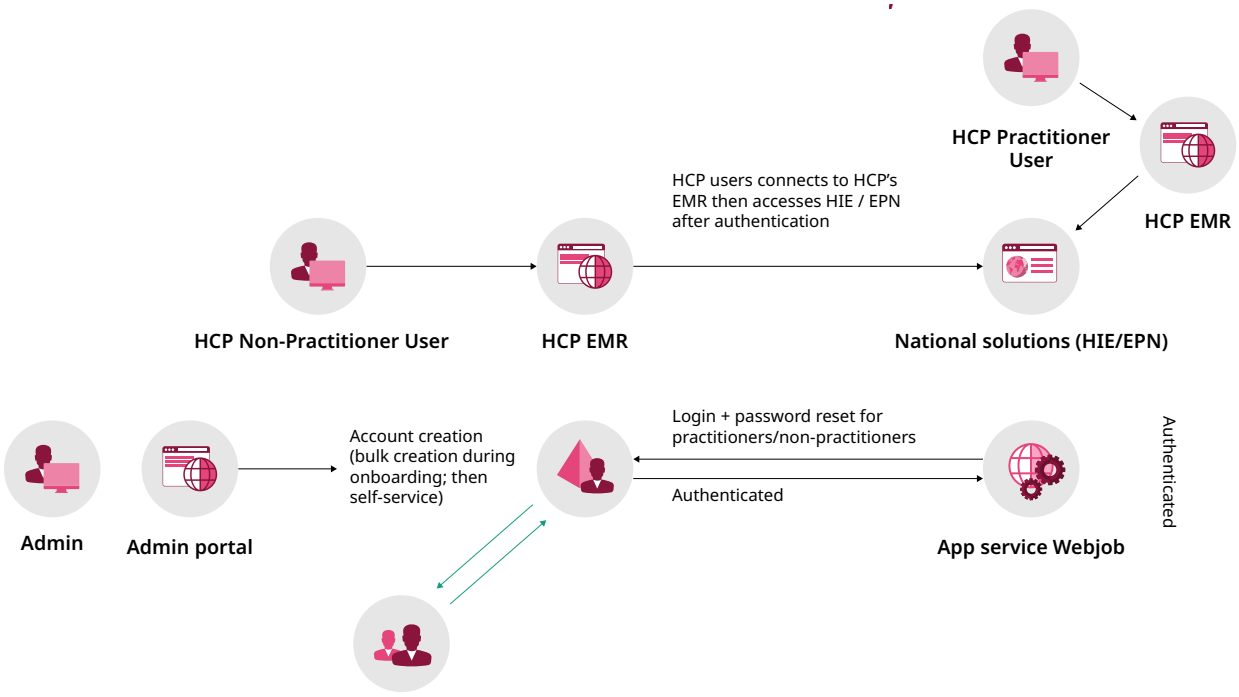


Figure 60. Healthcare provider Users onboarding and authentication flow

- Staff Type
- Solutions for which access is required
- Access Duration
- Object ID (from AD) resources

The above details can be provided in the Bulk User Creation Template. These users accounts will be created programmatically by the MoPH QHIE-Hub administration team.

Outlined below are the key steps healthcare providers need to follow for end-user identity creation:

1. Healthcare provider Identity Admin needs to fill out the Bulk User Creation Template (for both practitioner and non-practitioners) and submit it to MoPH or its affiliate stakeholders
2. For healthcare practitioners, the QHIE-Hub system will validate the practitioner's license against DHP; practitioner users who do not have a valid license will be identified and sent back to healthcare provider to correct
3. For the remaining correct users, MoPH will use the internal admin portal to bulk-create the local B2C accounts on the platform and assign the requested role
4. This will trigger a registration email to healthcare provider users with a registration link
5. The user needs to open the link from the registration email. They also need to verify their mobile number by receiving an OTP on the number shared by the healthcare provider in the template (for practitioners, this number must also be the same as the one in DHP).
6. If the user's OTP Verification passes, he/she will be asked to create a new password; then he/she can access QHIE-Hub portals using the newly created credentials.

Post onboarding, the user assigned the Healthcare Provider Identity Admin role can login to the QHIE-Hub healthcare provider Identity Management Portal and enter information to create new users/modify current users.

Note:

If the practitioner is using a number different than what is recorded in DHP, then he/she needs to update their number in DHP and retry completing the registration by clicking the link again.

They also need to manage accounts and offboard users leaving the organization. The QHIE-Hub will follow the same process of validating practitioner's licenses against DHP for eConnect/eMeds. A registration link and OTP verification will be triggered for new users. If the practitioner's

license is not valid, the Identity Admin will get an error message and this user will not be able to access QHIE-Hub solutions.

8.4.2 First-time login mechanism for practitioner users

As part of Go-live, healthcare providers must ensure that all practitioners can login to the QHIE-Hub solutions via the Health Information Exchange solution.

The process of signing into a user's account via Health Information Exchange solution has the following preconditions:

- The user must have an active license as a Practitioner.
- The user must have an active license record in DHP.
- The user must be registered with at least one organization as a Healthcare Professional in HPM.
- The user must have a registered account in the system (created by the respective organization)
- The user must have received a system-generated email from Azure B2C with login credentials

Steps to sign into the Health Information Exchange (HIE) Viewer for the first time:

To sign into the Health Information Exchange system:

1 Go to the link **https://hiev-ppr.MoPH.gov.qa/** and select "Local Account"

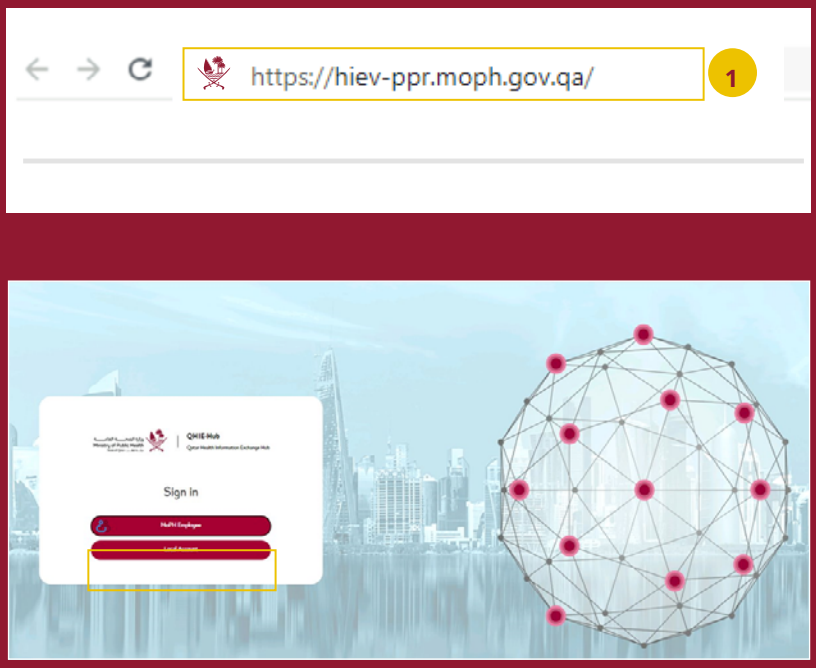


Figure 61: Link for HIE

2 Write your e-mail address and password provided by MoPH.

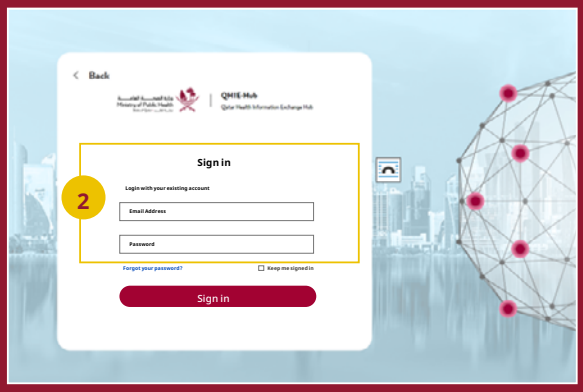


Figure 62: Login page

3 Click on the Sign in button.

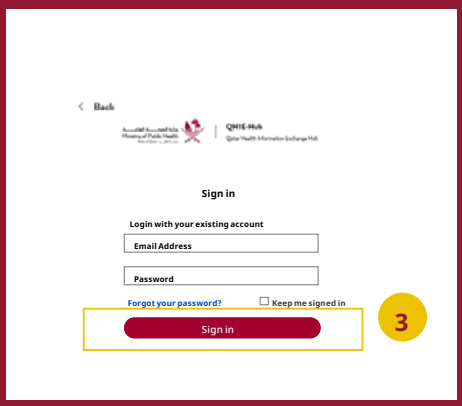


Figure 63: Login page

4 Choose the authentication method.

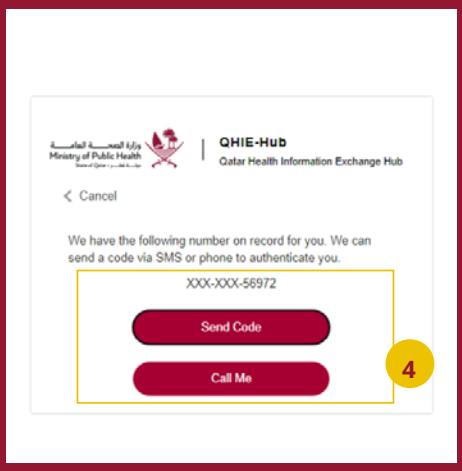


Figure 64: MFA login details

5 Enter your verification code.

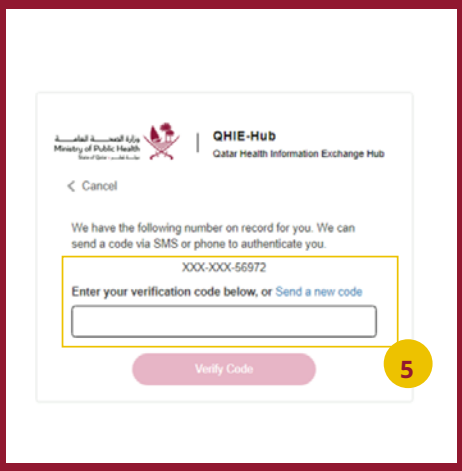


Figure 65: Verification screen

6 Click on the Verify Code button.

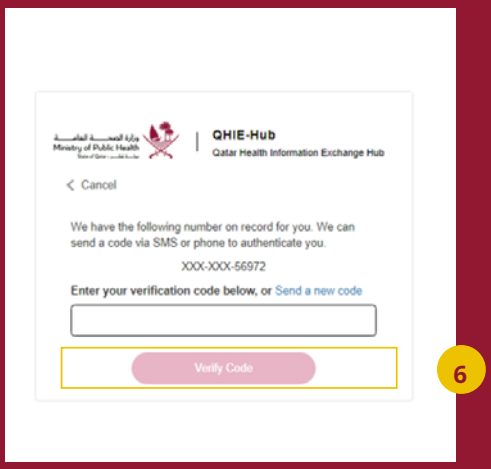


Figure 66: Verification screen

7 Password set up

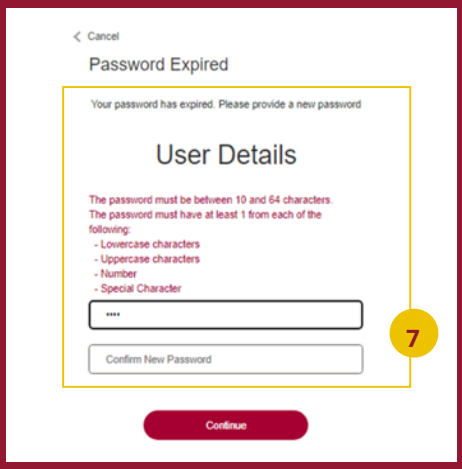


Figure 67: Password set up

8 Click on the Continue button.

The password provided by MoPH is only applicable for the first-time logins. The user must provide a new password and confirm the new password into the relevant fields. The password must be between 10 and 64 characters, and must have at least 1 from each of the following:

- Lowercase characters
- Uppercase characters
- Number
- Special Character

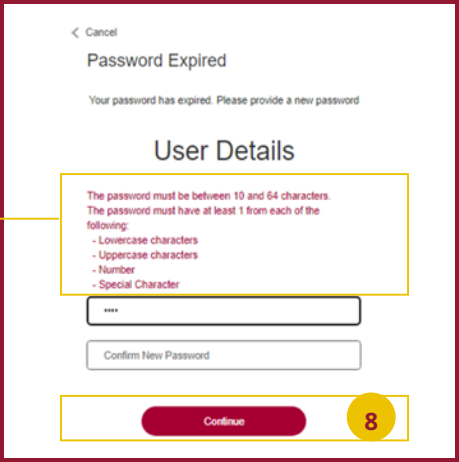


Figure 68: Terms and conditions

9 Click on the <<I agree to the Terms of Service<< checkbox.

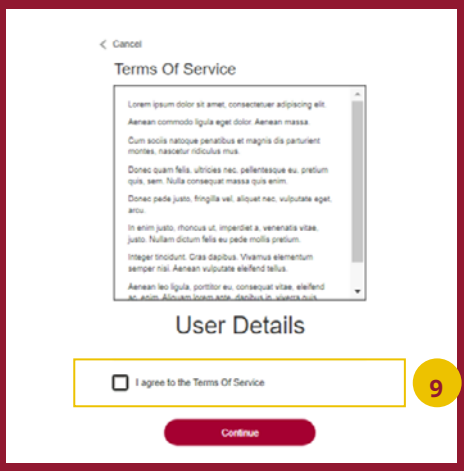


Figure 69: Terms and conditions

10 Click on the Continue button.

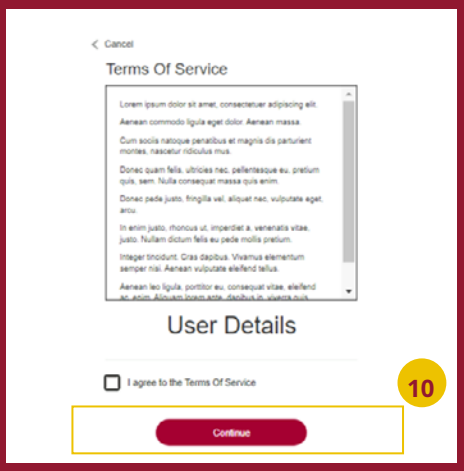
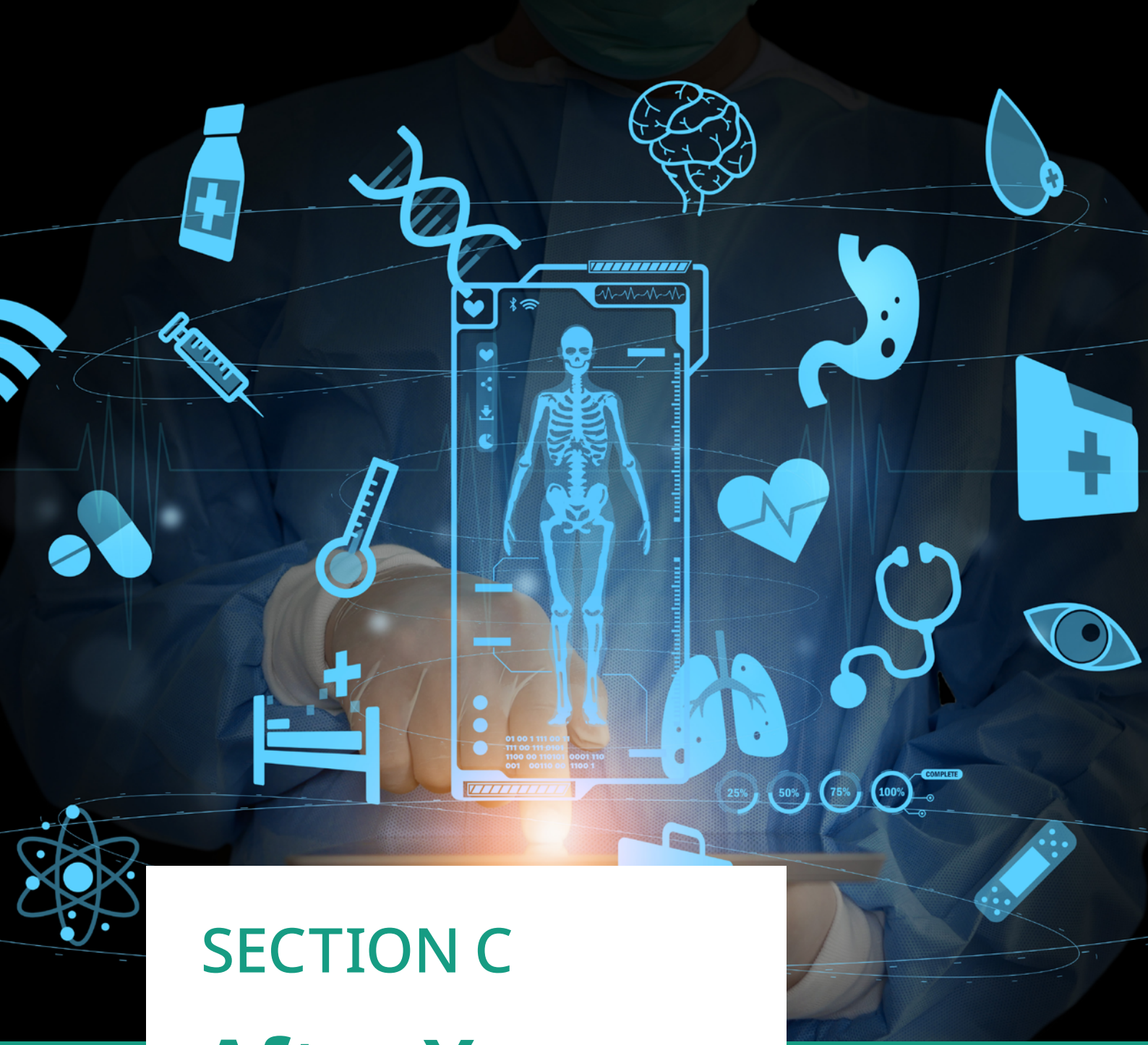


Figure 70: Terms and conditions

*****



SECTION C

After You Onboard


Mandate, policies &guidelines
Overview of national solutions
A. Get familiar with QHIE Hub
B. Get ready to onboard
Onboarding Roadmap
Implementation Plan
Change management
Meet requirements (security, integration, data)
Connect to sandbox to develop APIs
Map & transform data
Clean historical data
Validate patient demographics
Connect to Pre-prod to test workflows
Training
Complete onboarding assessment
Actual onboarding/production
Go live
GO LIVE
You are here
C. After you onboard
Drive adoption
Monitor data quality

CHAPTER 9

After You Onboard

9.1 Drive adoption and realize benefits

After onboarding to the QHIE-Hub, healthcare providers are required to drive adoption of national solutions across end-users (e.g., physicians, nurses etc.) by training them on new processes, increasing awareness about the benefits of the QHIE-Hub and planning other adoption interventions. Healthcare providers are also required to monitor adoption metrics and report them to MoPH periodically.

A healthcare provider's adoption strategy must focus on informing all users about the benefits/ features of the QHIE-Hub and must make usage of the national solutions part of normalized behavior of the users.

Healthcare providers are expected to develop their own adoption strategy for the QHIE-Hub solutions. It is recommended that their adoption strategy has four core components centered on user enablement as outlined in the figure 71:

Adoption strategies typically have three objectives:

- The **first objective** is informing users across all stakeholder groups (i.e., physicians, residents, pharmacists etc.)
- The **second objective** is scaling usage through the regular use by making the QHIE-Hub solutions the de-facto solution, part of normalized behavior for users.
- The **third objective** is maximizing value, whereby benefits of the solutions are realized. This will manifest in the form user satisfaction and attestation, leading to improved health outcomes

A healthcare provider's adoption strategy must have 4 core components centered on user enablement

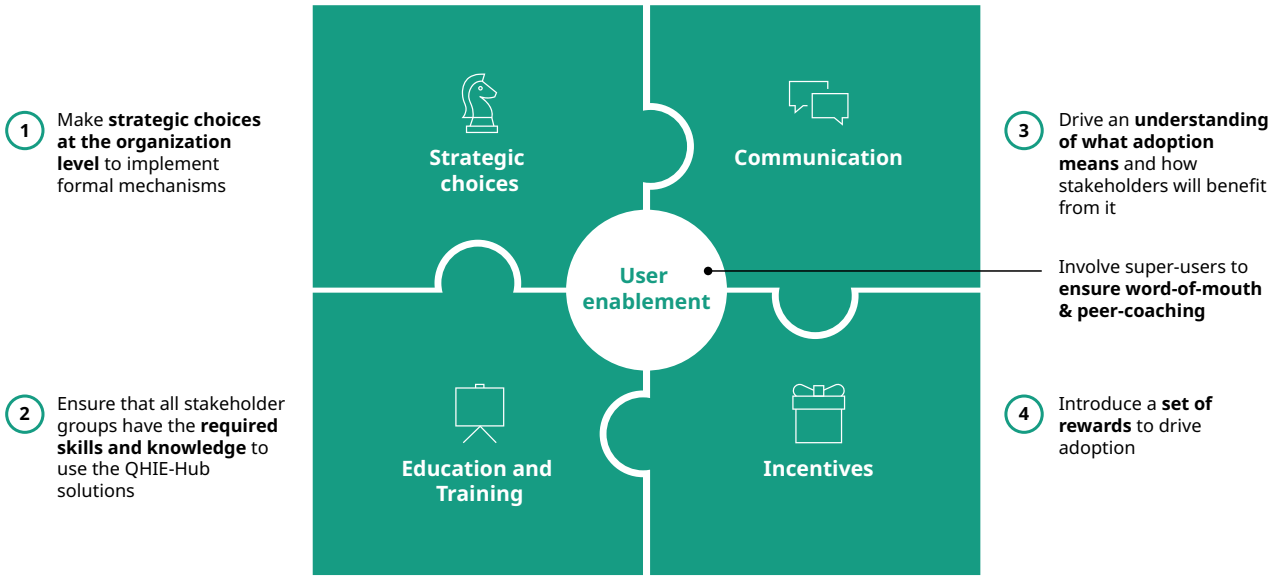


Figure 71. Components of an adoption strategy

Solution	KPI
QHIE-Hub Platform	% of patients registered/matched via eMPI v/s all patients registered
eMeds	% of staff who completed trainings
	% of active users (i.e., proportion of users using solutions v/s those eligible for use)
	% of prescriptions issued / dispensed through ePrescription and Digital Pharmacy
	User satisfaction score
eConnect	% of staff who completed trainings
	% of active users (i.e., proportion of users using solutions v/s those eligible for use)
	User satisfaction score
eCare	% of staff who completed trainings
	% of patients who received care that was consistent with guideline recommendations
	% of patients in the existing registries of healthcare providers, if any, added to the eCare
	User satisfaction score

Table 25. Indicative list of adoption KPIs

To track efforts, healthcare providers must define key performance indicators (KPIs) for adoption of the solutions. Below are a set of adoption and data quality KPIs that healthcare providers should monitor and report to MoPH:

Outlined below is an indicative list of initiatives that healthcare providers can plan to undertake (based on relevance and size) to drive adoption of the QHIE-Hub solutions:

One-to-many communications:

- **Town hall meetings:** After successful onboarding, healthcare providers can organize periodic meetings where the leadership emphasizes the importance of the QHIE-Hub, shares success stories, and addresses any concerns or feedback
- **Internal knowledge sharing workshops:** In addition to formal training programs carried out by the training coordinator with trainers, healthcare providers can also organize peer coaching sessions where employees can get further handholding and learn about the benefits or features of the national solutions from other users
- **Regular internal updates and newsletters:** Healthcare providers can also release organization-wide newsletters to share the latest updates, success stories, benefits etc. to keep employees informed and engaged

Internal champions & recognition:

- **Internal champions:** Healthcare providers may identify "QHIE-Hub Champions" within their organization across departments who can guide and assist their peers as they use the solutions
- **Recognition:** They can also carve out incentives and provide formal recognition to employees who actively use and promote the national solutions.

Feedback mechanism:

- **Suggestion box:** It is recommended that healthcare providers have a suggestion box or develop online forums where employees can provide feedback, suggestions, or raise concerns on how to use the QHIE-Hub national solutions. These may also be shared with MoPH from time-to-time as inputs to the future roadmap of the solutions

Implementing these initiatives will enable healthcare providers to actively promote the adoption of the QHIE-Hub solutions, leading to improved health outcomes and efficient healthcare delivery.

9.2 Understand release management

To ensure continuous improvement of national eHealth solutions, MoPH will perform periodic upgrades, while maintaining the integrity of the existing production environment.

To continuously improve national solutions, MoPH will release periodic upgrades. Healthcare providers are required to update their application instance to the latest version within the specified deployment timeline for every release.

This chapter defines the release management process healthcare providers need to follow once they are onboarded to the QHIE-Hub. It includes details that can help healthcare providers in planning, developing, scheduling, testing, deploying, and controlling applications releases.

Healthcare providers are required to update their application instances without fail after the QHIE-Hub releases a newer or upgraded version. The key activities they are expected to undertake across different phases of release management are outlined below:

Pre-release phase

- **Stay informed** – moph will develop a detailed release calendar and share it with healthcare providers in advance through different channels (such as e-mail, newsletters, etc.). Healthcare providers will also receive clear communications about upcoming releases, release notes, pre- and post-deployment timelines, warnings about potential downtime and system behavior changes when such updates/changes are rolled out. For certain urgent security fixes, healthcare providers may be notified at a shorter duration (at least 1 week in advance). Healthcare providers are expected to be up to date with this information.
- **Plan** – based on the information provided by moph about upcoming releases or security fixes and the respective release notes, healthcare providers are expected to plan the testing of these services in non-production systems along with the subsequent upgradation of their production systems. These must be scheduled in a manner that ensures minimal impact on day-to-day operations of the organization and zero impact on patient care."

Transition phase

- **Test** – All healthcare providers are expected to run parallel versions of applications in a non-production environment. Releases must first be installed in the non-production environment where the technical and business impact assessment of the changes must be ascertained.
- **Leverage support** – MoPH will continuously track the issues and monitor the impact of releases to ensure system performance, stability, and data security. In case healthcare providers face issues in making these upgrades, they may leverage the support channels for troubleshooting. These are detailed in the next chapter.

Post-release phase

- **Communicate to end-users** – After a release, healthcare providers are expected to promptly undertake change management efforts based on the degree of impact on existing workflows / systems. They must inform end-users about the latest changes and improvements. For this, they must create a communication plan that leverages one or more channels, based on the need and urgency of the update.
- **Document changes** – Comprehensive release notes will be provided to healthcare providers, outlining changes and improvements in a timebound manner. Healthcare providers must note these and must create their own internal release notes about the overall process of upgradation

Share feedback – Evaluation of the release will be carried out through a variety of methods such as surveys, interviews and focus groups. Healthcare providers are encouraged to participate in these to provide feedback and suggestions for ongoing improvements.

9.3 Leverage support & maintenance

To ensure that the QHIE-Hub national solutions can be used in a hassle-free manner, MoPH will provide extensive support across multiple levels. These levels include:

1. **User self-help and retrieve support** (includes support for basic issues such as email setup, FAQs etc. covering access to national solutions, permissions, and general use of system)
2. **Service desk support** (includes support for day-to-day troubleshooting requests across access issues, permissions, and technical support on applications)
3. **Infrastructure & application technical support** (includes access to experienced and knowledgeable technicians to assess and provide solutions on major issues related to infrastructure, applications, security, firewall etc.)
4. **Expert product and service support** (includes access to the highest technical resources available for problem resolution or new feature creation that focuses on the principal reason of the problem or issue, including potential issues in product design, programming, or configuration of the solutions).

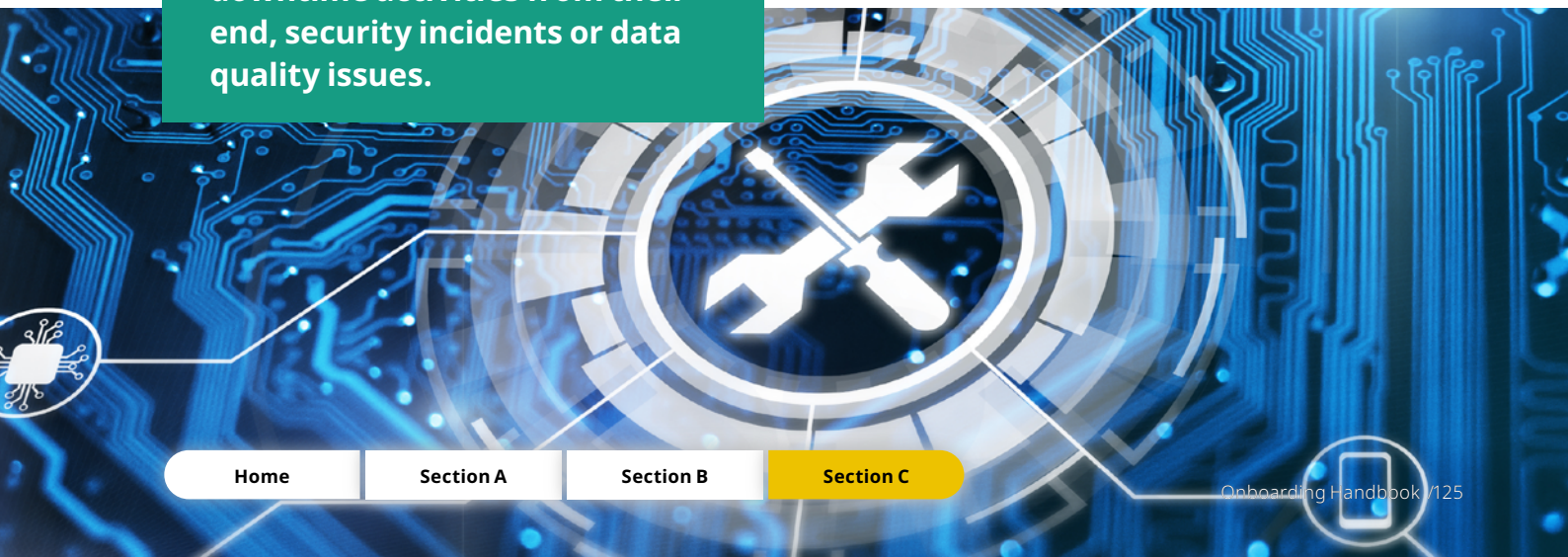
For continuous support, the QHIE-Hub has setup a 24/7 telephone helpline and email. Healthcare providers may leverage these to raise tickets or to report planned or unplanned downtime activities from their end, security incidents or data quality issues.

Healthcare providers can engage support through two channels – both as part of their onboarding and after they are onboarded. They must nominate a Service Manager who will be responsible for coordinating with MoPH support teams on critical issues.

The service manager will be responsible for the following activities:

- Act as the first point of contact for all internal users in case of support issues/incidents
- Liaise with MoPH support teams for reporting & escalating incidents/issues by using the defined communication channels (i.e., phone/ e-mail)
- Intimate the support team in any case of downtime and to escalate if resolution is not done on time
- Co-ordinate and ensure implementation of mitigation activities towards any incidents that may need to be undertaken on healthcare provider's network/environment
- Ensure application instances are updated without fail after the QHIE-Hub releases a newer or upgraded version
- Engage with MoPH during release management for providing status and seek any support as needed
- Liaise with the QHIE-Hub, all regulation authorities, national and local law enforcement, and other jurisdictional authorities in case of security incidents / breaches

Following are the support channels that will be operated by MoPH to address any issues faced by healthcare providers while using the QHIE-Hub solutions or in case they need to report planned or unplanned downtime activities from their end, security incidents or data quality issues:



1. Telephone helpline

A dedicated telephone helpline **(XXXXX)** can be used to raise queries and troubleshoot issues related to the QHIE-Hub applications and infrastructure services. This will be the primary channel and will provide timely assistance to healthcare providers and their users.

The helpline operates during the following working hours:

- **24x7x 365 for the critical incidents**
- **Standard incidents during the working hours**

2. Email

Healthcare providers or service manager can also email the QHIE-Hub at **[xxxxx@MoPH.gov.qa]** to raise support tickets or to report issues.

Issues/incidents raised across both channels will be accompanied by a ticket number that needs to be quoted for all follow-up communication. Healthcare providers must leverage the above-mentioned support channels to report any planned or unplanned downtime activities from their end, security incidents or data quality issues.

Information needed

A healthcare provider must provide the below information when contacting the support desk to raise a support ticket.

It is recommended that all end-users contact their service manager first to report issues/ incidents. The service manager is expected to evaluate the issue to determine whether it is a known or an organization-wide issue (where a support ticket already exists) or a new issue where a ticket needs to be raised. They are also expected to help the end-users with common fixes if it is a known issue.

Based on this preliminary evaluation, a new support ticket may be raised either by the service manager (recommended option, particularly if the issue impacts multiple users) or by the end-user via the QHIE-Hub support helplines.

Issue Log Field	Description
User information	Healthcare provider's name, role of the user, and contact details
Date identified	Date on which the issue was identified
Issue description	Description of the issue and the application which was impacted
Impact (clinical/business & technical)	Clinical impact/business and technical impact along with number of users impacted (if available); highlight if patient care is being impacted
Steps to re-create issue	Details on how the issue was encountered or detected by the users
Error message (if any)	Details of the error message being encountered
Attachment (if available)	Screenshot of the error message being encountered
Mode of usage (if known)	Standalone or integrated
Related issue ID (if available)	Documentation of any other pervious and/or existing issue (if applicable)
Severity (standard/critical)	**Internal classification of the severity** of the issue that determines the SLA for the resolution

Table 26. Issues Log Template

Response time

1. **Critical issues:** These are issues that significantly impact business operations or system functionality and require immediate attention. The typical response time is within 30 minutes of receiving a critical issue report. Depending upon the severity of the issue, the resolution time can be within 2 - 4 hours. Complex issues that involve in-depth investigation or consultation with multiple stakeholders may take longer to resolve. An expected resolution time will be communicated at the time of raising the complaint.
2. **Standard issues:** These are non-critical issues that may affect user experience but do not have an immediate impact on patient care. The target response time is within 1 – 2 hours and the resolution time is within 6 – 8 hours.

Escalation procedure

If an issue is not resolved within the specified resolution time or requires further attention, it can be escalated using the same email address as mentioned above. The complainant will be informed of the escalation process and timeline. Periodic updates will be provided to the complainant until the issue is resolved to their satisfaction.

Communication schedule:

- Healthcare providers will receive periodic updates on the resolution status of the incidents raised by them until the issue is resolved.
- Planned maintenance and downtime notifications will be sent at least 72 hours in advance before the release of any changes. A reminder will also be sent 24 hours in advance to the healthcare providers / service managers. These emails will provide information on the estimated timeline for completion of the maintenance activities and a status update once they are completed.
- In the unlikely event of an unplanned downtime, all healthcare providers / service managers will be promptly informed about the nature of the issue, its criticality, mitigation plan and the estimated resolution time by when the application / infrastructure will be available. In all such scenarios, email will be the primary mode of communication. Additional details on how healthcare providers can mitigate the situation will be shared as and when such an incidents occur.

Reporting and follow-up

The QHIE-Hub will maintain a records of all grievances, including acknowledgment, investigation, resolution, and follow-up actions.

Once a support ticket is closed, an automated email with a short survey will be triggered to capture the feedback on the resolution. Healthcare providers are encouraged to fill this to continuously improve the overall support experience.

9.4 Create a business continuity plan

All healthcare providers must have a business continuity plan for contingency situations. Day-to-day operations may be impacted by unplanned downtime arising due to a connectivity failure, unavailability of the QHIE-Hub solutions or select services, or due to a failure in updating the application instance (both at MoPH or the healthcare provider's end). Healthcare providers may also have planned downtime due to scheduled maintenance activities. In all these scenarios, a business continuity plan is essential.

The guiding principle that healthcare providers need to follow is any planned or unplanned downtime must have minimal impact on day-to-day operations of the healthcare provider and zero impact on patient care. Hence, they must develop a business continuity plan that covers the following requirements (at a bare minimum):

- Availability of normal (offline) registration of new patients and patient search within the local patient database in case the QHIE-Hub platform or the eMPI service is unavailable
- Prescription/dispense of medicines via existing systems in case eMeds is unavailable
- Display of patient medical history based on medical records within the hospital in case Health Information Exchange is unavailable
- Backup of all patient and hospital data (including but not limited to data across FHIR profiles in the format prescribed by the Target datasets) for disaster recovery scenarios
- Implementation guides / documentation to deploy the QHIE-Hub solutions (including

configuration changes made in the local systems/EMRs) for disaster recovery scenarios

In addition to the above requirements, a healthcare provider's business continuity plan must address two possible scenarios:

1. **In case the QHIE-Hub services are unavailable:** Healthcare providers are expected to continue business-as-usual. They must also continue sending the FHIR/HL7 messages that will be stored in the QHIE-Hub pipeline and will be processed as soon as the QHIE-Hub systems are back online. However, if a healthcare provider is unable deliver messages to the QHIE-Hub (i.e., there is an error/failure while sending the message), they must note the time of the last sent message and must retrigger all messages thereafter, as soon as they receive a notification from the QHIE-Hub about the restoration of services.
2. **In case there is unplanned downtime or scheduled maintenance at the healthcare provider's end:** Healthcare providers must proactively notify MoPH about the duration of this downtime, scope of maintenance activities with other relevant details via the support helplines (particularly if it is likely to impact or delay the transmission of patient information from their end). In all these scenarios, the provider must note the exact duration of this downtime, update their digital records and retrigger messages that were not sent in this period once their systems are restored.

9.5 Report security incidents and issues

This section explains the actions healthcare providers are expected to undertake in case of security incidents / breaches at their end. In all such situations, it is imperative that the service manager of the respective healthcare provider shares immediate information with the QHIE-Hub as soon as any breach within their organization is detected. This will enable the QHIE-Hub to take timely actions aimed at safeguarding patient information across the full ecosystem.

- In the event of a security breach or data leakage, healthcare providers are required to proactively and immediately inform MoPH, National Cyber Security Agency (NCSA), and National Data Privacy Officer (NDPO). These breached include both those within the organization and those via third parties that may have a connection to the healthcare provider's network.

Healthcare providers are required to proactively and immediately report any security incidents/ breaches as soon as they are detected to MoPH, NCSA and NDPO.

- The service manager must be the single point of contact who liaises with the QHIE-Hub, all regulatory authorities, national and local law enforcement, and other jurisdictional authorities. Based on guidance from these stakeholders, the service manager will be responsible for coordinating and ensuring mitigation activities are implemented.
- All healthcare providers are expected to develop an incident response plan and a detailed playbook in advance. As soon as an incident is detected, healthcare providers need to execute remedial measures as outlined in their incident response plans.
- Any connections between the third parties' network and healthcare provider's corporate network must be terminated in case of a security breach or in case of non-compliance of the third party with a healthcare provider's own security policies.

*****

CHAPTER 10

Continuous Governance

10.1 Monitor data quality

Achieving and maintaining high quality data is critical to MoPH and the QHIE-Hub's strategic objectives. It enables:

- Better health outcomes and more efficient care for patients vis-à-vis potential risks to patient safety due to inaccurate, incomplete, or delayed health data
- Higher confidence and benefits realization for the overall health sector in the State of Qatar
- Improved quality of decision-making across public health policies and increases credibility of medical research

All HCPs are required to monitor the quality of their data, detect data quality issues, and take mandatory steps to resolve them. This includes logging, tracking and remediation by undertaking a root cause analysis and by implementing fixes.

For these reasons, all healthcare providers are required to consistently monitor the quality of data generated by their source systems against the data quality criteria such as uniqueness, validity, accuracy etc. that are outlined in Chapter 6.3 Data.

As part of continuous improvement, MoPH will also monitor and report data quality issues to healthcare providers as and when they are found. Communication on these issues will be done via the support team. Healthcare providers will also receive error messages if the data being sent has been rejected by the QHIE-Hub due to non-conformance with the target datasets / value sets or the pre-defined business rules.

In all the above cases, healthcare providers are required to note the issue, undertake a root cause analysis to mitigate it and report back on the mitigation status within a defined timeline. They must fully resolve the data issues before re-loading or re-sending the data to the QHIE-Hub (rather than continuing to send erroneous data). They must also re-trigger the rejected messages for the duration when the data quality issue persisted and when errors were being reported.

Define data quality KPIs and evaluate the data

Healthcare providers must evaluate their data for compliance with pre-defined KPIs as outlined by MoPH, develop additional KPIs, set internal targets for them and track them. These KPIs must be specific, objective, in alignment with clinical practice, and measurable with automated tools.

The Table 27. shows examples of KPIs that can be utilized with along with the applicable data quality criteria, domain, and target:

A detailed set of data quality rules and KPIs are given as part of the reference documents along with the onboarding handbook.

KPI	Data Quality Criteria	Domain	Target
Percentage of duplicate Encounter IDs	Uniqueness	Encounters	=0%
Count of encounters post-death	Plausibility	Encounters	0

Table 27. KPIs Example

Monitor KPIs and detect issues

Once the data quality KPIs and targets are set to the applicable domains, healthcare providers need to periodically assess their data against the KPIs within pre-defined timelines. The detected issues must be logged, tracked, and reported to MoPH during the Post-onboarding Review. A detailed template for this review will be shared six months after the onboarding of a healthcare provider.

Each healthcare provider needs to maintain their own data quality detection mechanisms / tool to ensure effective monitoring of data quality. Few examples of such detection mechanisms are outlined below:

- **Dashboards** – The first and easiest mechanism to detect data quality issues is through an automated dashboard that monitors the data quality against the data domains and KPIs.
- **Alerts** – Alerts can be set up to avoid human dependency and to trigger notifications when there is a sudden / significant drop in quality for a specific KPI.
- **Audits** – Audits can be performed to evaluate point-in-time quality of data, availability of tools / processes and performance against best practices. They are usually completed by a staff member or consultant who has professional training, education, or experience.

Once healthcare providers have detected data quality issues, there are 2 key steps they are expected to take.

1. Logging and tracking

All data quality issues must be logged by healthcare providers so they can be tracked to closure and avoid being forgotten or discarded. Logging data quality also enables healthcare providers to find trends in data quality to identify common failure points in the data or systems. It is important to note that data which is not fully compliant with MoPH business rules will be rejected by the QHIE-Hub platform. These issues must also be logged and tracked internally.

Logging and tracking data quality issues must be done centrally through an issue management tool. For each identified data quality issue, it is recommended that the below fields are captured and updated as the investigation and remediation of the issue progresses.

All data quality issues that impact the accuracy of a patient record or hamper the healthcare provider's ability to send data to the QHIE-Hub (irrespective of the number of patients) must be reported to the QHIE-Hub via the support helplines.

2. Remediation

Once a data quality issue is detected and logged, it must be remediated by identifying the root cause and by implementing fixes.

a. Root cause analysis:

This step involves understanding the issue's fundamental cause and solving it at the source, as opposed to fixing where the DQ issue surfaces or manifests. Identifying whether the cause of the error is a systemic issue, or the result of a one-off event (e.g., one time data entry) is critical so that the right measures and

Issue Log Field	Description
Issue ID	Unique identification number generated (manually or automatically) for the DQ issue
Issue status	Status of the data quality issue
Issue description	Description of the data quality issue
Priority (P1, P2, P3)	Priority of the data quality issue
Reported by	Name and contact details of the person who reported the data quality issue
Detection mechanism	How the data quality issue was reported / steps to recreate the issue
Issue owner	Name and contact details of the issue owner
Date identified	Date on which the data quality issue was identified
Last update date	Date on which status of the issue or any of its attributes was modified
Related issue ID	Documentation of any pervious and/or existing data quality issues related to the current issue
Location of DQ Issue	Location where the data quality issue was discovered (database name, table name, field name, system name, etc.)
Root cause	Identified source/reason for the data quality issue based on investigation
Clinical impact	Details of clinical or patient impact of the data quality issue on business
Technical impact	Data transfers to QHIE-Hub impacted by the DQ issue

Table 28. Recommended data quality issues logging template

resources are deployed to fix the issue. Once the root cause is found, it is recommended that it is documented in the issue log template. Common root causes of data quality issues include:

- Manual entry error: for example, a 'typo' error or data placed in the wrong data fields (e.g., entering the value of height in the weight data field)
- Incomplete or missing data: for example, some critical data fields have not been populated (e.g., vital signs are not entered) or are being captured due to workflow / system limitations
- Non-compliance: for example, a data quality rule was not followed when creating or updating data (e.g., laboratory codes are not in the LOINC standard)
- Incorrect mapping during migration or transformation: for example, data from a legacy system has not been migrated into the correct data fields of a new system (e.g., migrating from one EMR system to another)
- Data corruption due to technical or network level issues

Effective action to address the data quality issue can only be taken if the root cause of the data quality issue is well understood and identified. Root cause analysis ensures treating the cause of poor data quality, rather than the symptoms.

b. Implementing a fix:

The actions taken to remediate the data quality issue depend on the root cause of the issues that have been identified. Common data quality remediation actions include:

- Introducing automated data quality checks for data entry, such as data validation (e.g., the EMR checks for a correct value for the vital signs)

- Improving training and guidance for those involved in data entry (e.g., training of reception and different departments' clerks, nurses, and clinicians)
- Applying additional automated data quality controls during data transformation, mapping, storing or transmission

10.2 Enable Data Governance

Post onboarding, it is recommended that healthcare providers adopt best practices within data governance. This will ensure the sanctity of the data being sent by the healthcare provider to the QHIE Hub. A robust data governance framework has measures across three pillars i.e., people, process, and technology. This section provides recommendations for these areas.

3. People

In line with the future requirements of the QHIE-Hub, it is recommended that healthcare providers build capabilities or partner with technical vendors to acquire skills within the following areas:

- **Data stewardship** – Ability to manage the overall quality of clinical and non-clinical data in the organization and to develop processes that support all stakeholders in the identification and rectification of data quality issues
- **Data analysis** – Ability to analyze new requirements (e.g., standards, quality rules, policies) and coordinate with stakeholders to translate business needs to system rules
- **Data architecting** – Ability to define policies, procedures, and technologies that will be used to collect, organize, store, and retrieve data and to ensure adherence to national and eHealth standards / policies
- **Data engineering** – Ability to execute processes / techniques related to the exchange of data and to prepare data for analytical and operational use while ensuring compliance and regulatory requirements are met

Healthcare providers may be required to hire new roles within their organization such as data architects, data engineers, analytics experts, integration specialists etc. to build these capabilities.

4. Process

It is also recommended that healthcare providers follow best practices to institute key processes that ensure data is generated and managed efficiently within their organization. These processes must also enable compliance with national policies (e.g., MCIT data security policies, data classification policies etc.). Examples of a few processes include:

- **Conduct data architecture reviews:** Healthcare providers must conduct a detailed data architecture review to define their organization's strategic data needs, standards, infrastructure and determine integration points to meet these standards and quality parameters.
- **Develop data change management policies:** Healthcare providers must also define how they handle the data changes related to services / technology products by careful planning, assessment, design, implementation, and communication of these changes.
- **Monitor data operations:** Healthcare providers are also expected to define a process to monitor the development and maintenance of the data for all stakeholders by focusing on database support activities or data technology maintenance activities.
- **Maintain data security:** Healthcare providers are expected to periodically plan, develop, and enforce security procedures / policies to maintain proper authentication, authorization, access, and audit of data assets.
- **Master and reference data management:** Healthcare providers are advised to implement a framework that defines how their organization will execute the ongoing reconciliation and maintenance of master data and reference data to ensure consistency, accuracy, and relevance to the business needs.
- **Metadata management:** Healthcare providers are also advised to implement a metadata management framework that outlines how their organization creates, stores, integrates, and controls data definitions (data about data) and data cataloguing within the organization.
- **Maintain data quality:** Healthcare providers are advised to define how their organization

ensures data usage fitness by maintaining existing business rules, creating new data quality rules, metrics, and service levels for regular data monitoring, while addressing the data quality issues, as and when noticed.

5. Technology

Complying with the requirements of the QHIE Hub may also necessitate use of tools to carry out business operations (e.g., issue tracking, data cataloguing, workflow management, automation etc.) as well as database operations (e.g., database housekeeping such as tuning, profiling etc.). It is recommended that healthcare providers shortlist and deploy the necessary tools as required from time-to-time.

10.3 Data change management for the QHIE-Hub

To meet the Ministry of Public Health's strategic data needs and new or emerging requirements of its national solutions, the QHIE-Hub will collect data for specific use cases. It may also update its target datasets, value sets, data standards, terminologies, etc. from time-to-time to meet clinical needs or to comply with best practices. All such updates related to the QHIE-Hub data requirements will be part of the overall release management process outlined in Chapter 9.2 Understand release management.

All healthcare providers are required to take note of these changes and become fully compliant with them. They must follow the established release management process and complete all activities across the pre-release, transition, and post-release phases to ensure these changes do not disrupt day-to-day operations.

An indicative list of changes in the QHIE-Hub data repository that are likely to impact healthcare providers include:

- Updates in target datasets (e.g., addition of new FHIR profiles, addition of new elements within FHIR profiles, change of mandatory/must-support/optional categories)
- Updates or changes in the value sets, codable concepts etc.
- Changes in data terminologies/standards
- Addition of new data requests (e.g., non-clinical/administrative data)
- Changes in data models/architecture/structure or other common data requirements

All healthcare providers will be informed in advance about these changes through different channels (such as e-mail, newsletters, terminology management portal etc.). As outlined within the release management section, healthcare providers are expected to first install these changes in their non-production environment, conduct a detailed impact assessment of these changes, carry out integration/regression testing before upgrading their production systems.

The healthcare provider's designated data liaison will continue to function as the key communication link between a healthcare provider and the QHIE-Hub for the implementation of these changes by engaging the necessary business and technical teams behind the scenes.

If any issues arise related to the target data set implementation, the data liaison must leverage the support and maintenance helpline to raise the grievance with MoPH along with the magnitude of the issue at the healthcare provider's end.

*****

www.moph.gov.qa /MOPHQatar /MOPHQatar /MOPHQatar