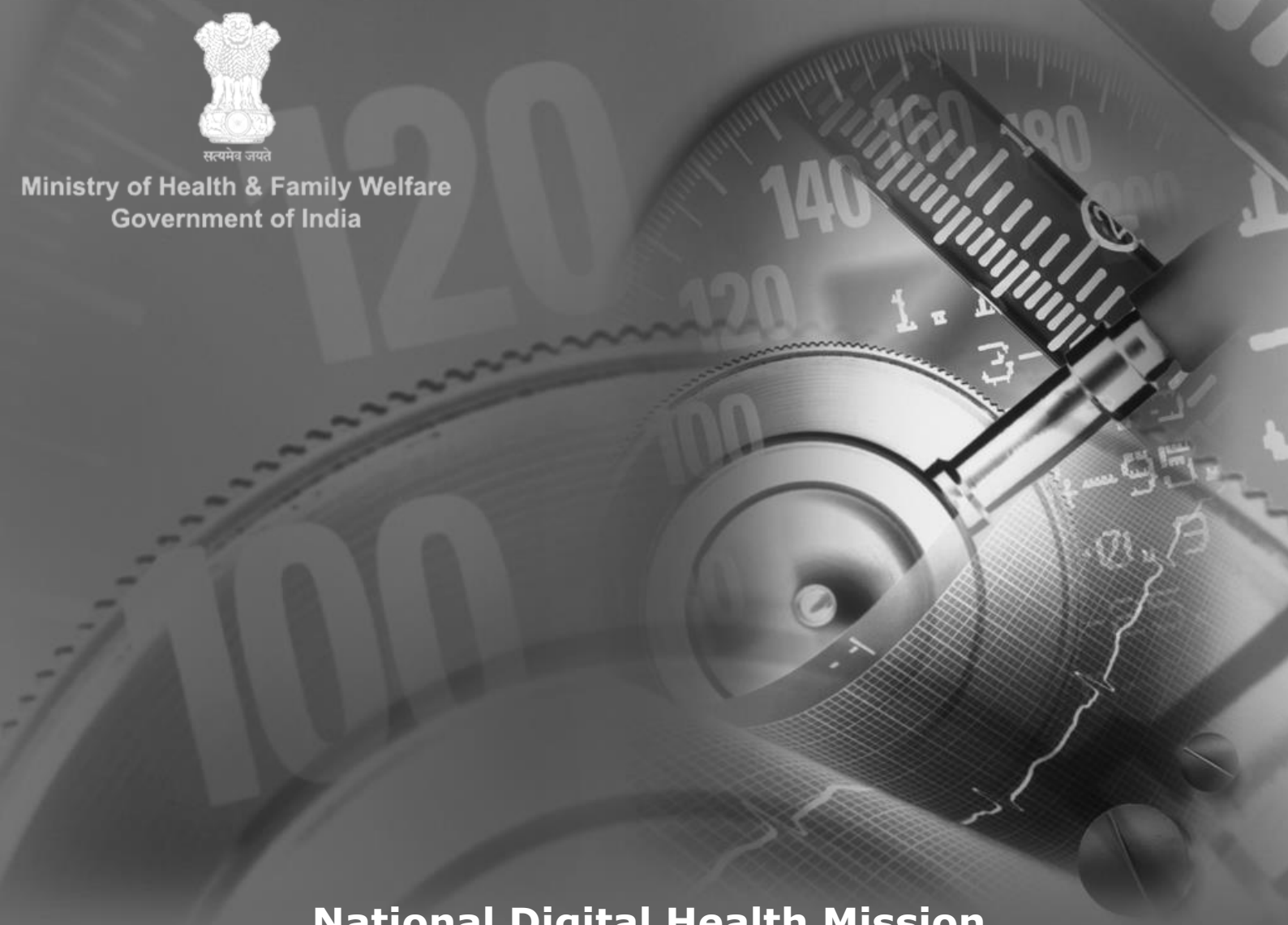


सत्यमेव जयते

Ministry of Health & Family Welfare
Government of India

National Digital Health Mission

Guidelines for Health Information Providers, Health Repository Providers, Health Information Users and Health Lockers

August 2020

सत्यमेव जयते national health authority

1 Summary

The National Digital Health Mission (NDHM) is working on bringing interoperability for digital health data in India. NDHM will manage the foundational digital building blocks that need to be adopted by all healthcare providers in the country.

Any Healthcare provider who is creating health data (diagnostic reports, discharge summaries, prescriptions, etc) digitally should participate in NDHM. They will be able to share these records with the patients and also fetch records issued by other providers with user consent.

Obtaining these benefits from NDHM requires the hospital / lab information management system or electronic medical record software that is being used by the healthcare provider to be upgraded to become NDHM compliant. The software being used by the provider must integrate with the digital building blocks of NDHM and comply with the guidelines outlined in this document. Healthcare providers are required to check with their vendor or inhouse software team and ensure they are working with NDHM compliant software.

The NDHM sandbox has been setup to enable any software to integrate with the digital building blocks and test their compliance to the guidelines and digital health standards. The sandbox offers all the Open APIs available under NDHM. Healthcare software developers are required to apply on the sandbox website (sandbox.ndhm.gov.in) for access. Full documentation on the Open APIs, a discussion forum for support, a hosted environment containing the digital building blocks and a test harness that will check for compliance is available at the sandbox.

NDHM requires the software be certified for compliance. NDHM will notify the agencies who are empaneled to certify the software is compliant to NDHM requirements. This is required to ensure correct capture and linking of health ids, secure storage of health data, use of standards in data exchange, etc.

Once a healthcare provider has access to a compliant NDHM software, they need to sign up in a NDHM registry to participate in the NDHM ecosystem. They will receive a set of digital keys that need to be configured in their NDHM compliant software.

With these access key and adoption of the NDHM compliant software at their facility, the healthcare provider will be able to register and issue Health IDs, issue health records digitally to patients and request and view patient's medical history with their consent.

2 NDHM Digital Building Blocks

The following are the core NDHM digital building blocks that enable an interoperable ecosystem

1. **Health ID:** Every person who wishes to participate in the digital health ecosystem must start by getting a Health ID. These IDs can be obtained via self-registration at healthid.ndhm.gov.in or from a PHR mobile application or at any participating healthcare provider. It is recommended that each person should have only one Health ID and they must provide it to their healthcare providers during their visit. Health IDs can be optionally linked to Aadhaar. Several Government schemes may accept only Aadhaar linked Health IDs.

2. **DigiDoctor:** NDHM maintains the national directory of all doctors and enables them to participate in the digital health ecosystem by enabling eSign for prescriptions, discharge summaries, clinical notes etc. All doctors at healthcare providers that are participating in NDHM are required to enroll at DigiDoctor (doctor.ndhm.gov.in). NDHM is also developing the health workforce registry covering all other healthcare workers and this will be available in the future.

3. **Health Facilities Registry:** NDHM maintains the national directory of all healthcare facilities. Any participating facility needs to sign up in the health facility registry at facility.ndhm.gov.in This ensures they are valid facility that is authorized to issue health records in the ecosystem

4. **Consent Manager and Gateway:** The exchange of health information is enabled by the consent manager and gateway. Health records can only be issued / viewed with patient consent. The consent manager supports requests, grants and revoking of consent by users.

There are several entities in the ecosystem that can integrate with the above building blocks

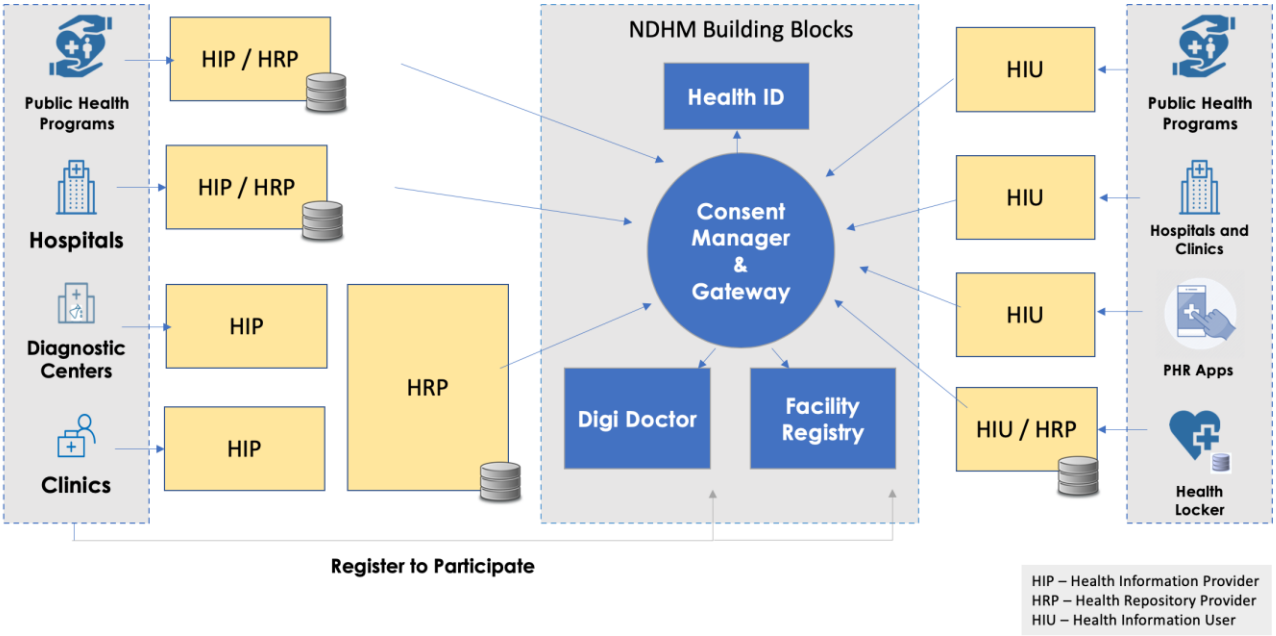
A. **Health Information Provider (HIP) –** Any healthcare provider who creates health information in the context of providing healthcare related service to a patient and agrees to share the same digitally with the patient using the consent framework adopted by NDHM is called a health information provider (HIP). All hospitals, diagnostic centers, clinics, public health programs, telemedicine players, etc are encouraged to become HIPs. HIPs use a NDHM compliant software that implements the HIP software specifications. The specifications are published at the NHDM Sandbox website.

B. **Health Information User (HIU) -** Any entity that would like to access health records of a individual is called a Health Information User. This would include hospitals / doctors who would like to view medical history of patients, mobile applications that want to display health data to users including Personal Health Record applications, etc. Access to Health data is available to a HIU only with the individual's consent. HIUs use a NDHM compliant software that implements the HIU software specifications. The specifications are published at the NHDM Sandbox website.

C. **Health Repository Provider (HRP) -** Health repository providers are software service providers who offer NDHM compliant software and long-term record storage to hospitals, diagnostic centers and clinics. The HRP service enables healthcare providers to become HIPs or HIUs and meet their obligations of sharing and securely maintaining health records of patients digitally. HRPs offer long term storage of health records on behalf of a HIP. For example, a hosted lab information management system provider (LIMS) may update their software to become a NDHM compatible Health Repository Provider. Any lab using this LIMS software can rapidly become a HIP by adopting the software.

D. Health Lockers – Health Lockers are software service providers who offer long term storage of records to induviduals. Health Lockers behave like HIUs when they are receiving health records of the user from healthcare providers. Health Lockers behave like an HIP when the individual shares his records from his Health Locker. Apart from Health records from recognized healthcare providers, Health Lockers also can store user uploaded health records.

The following diagram describes the NDHM building blocks and entities involved in exchange of health information with user consent.



A large hospital or a public health program (like RCH) could hold the records of patients in long term storage on premises or in the cloud as per its own policies. These hospitals will play the role of both HIPs and HRPs in the ecosystem

Smaller diagnostic centers / clinics may use a specialized health repository provider who provides software solutions to help issue documents to patients and hold the same in long term storage. The

software provider plays only the role of the HRP and supports the healthcare provider to become a HIP and participate in the NDHM ecosystem.

If a Hospital / Clinic wants to access the medical history of a patient, they need to become a HIU and comply with the guidelines for the same. Consumers can use the PHR mobile applications to view their records and also manage their consents. These applications also need to meet the HIU guidelines.

3 Guidelines for Health Information Providers

All healthcare providers are expected to become Health Information Providers over time. They must share a digital copy of any health report they currently provide as a physical printout and/or handwritten records to the user via the NDHM architecture. Any Hospital, diagnostic center, clinic, public health program, etc. creating digital health records for patients can become a HIP by signing up with the NDHM registries. The registry will issue them a digital key that needs to be configured in the application, being used by the facility, that is certified to be compliant with NDHM standards.

3.1 Obligations of a Health Information Provider

Healthcare providers commit to the following when they agree to become HIPs

1. **Collect Health ID during registration –** As Health IDs start to get widely adopted, HIPs must check with Patients if they have a Health ID. If they do, then the HIPs must capture and validate Health IDs at the point of patient registration. The process to be followed for correct **capture and verification** of Health IDs is outlined in the documentation on the NDHM Sandbox website. HIPs understand that this process is **voluntary**, and they will not force any patient to provide a Health ID if they do not want to share it.

2. **Issue Health IDs to interested Patients** – HIPs are expected to educate patients and help create Health IDs for those that require assistance. Several sections of society, which include the elderly population, illiterate users etc, will require assistance in creation of Health ID. Aadhaar linked Health IDs can be created for those that do not have a mobile phone. It is recommended that a printed Health ID card is provided to these patients to ensure they can use this card across multiple health institutions. If a Hospital is already issuing a patient registration card, it is encouraged to include the Health ID No and the Health ID QR code on its existing cards. This integration can be achieved using the Health ID Open APIs. The process for issue of Health IDs is described in section 3.2

3. **Link the Health ID to their health records and notify on new records** – HIPs must store the Health ID collected and verified along with any health records they have created and are creating for the patient. HIPs are expected to continue to have their own provider issued patient id and only link the Health ID in their systems from those users who voluntarily provide the Health ID. When a new health record is generated for a patient, HIPs notify the same directly to patients via sms or via the consent manager. The process in described in in the documentation on the sandbox website

4. **Operate a HIP service –** The HIP service is an online system that responds to data requests from the consent manager. The HIP service must be compliant to the NDHM Open APIs. The service is designed to ensure that sharing of any Health records is only possible after validating the patient's consent. Any record shared must meet the minimal health data interchange

standards. These standards are designed to allow the HIP to start issuing records in existing formats (like PDF) and migrate to structured health data formats in FHIR over time. The HIP service also needs to meet the security and privacy guidelines specified by NDHM. The service must offer high uptime and availability. The NDHM infrastructure uses a set of heartbeats to measure the uptime of the HIP service. All HIP services must first integrate with the NDHM Sandbox and undergo a certification to be enabled on the NDHM network. If a facility with on premise software wants to play the role of both HIP / HRP – they must setup an infrastructure with a reliable connectivity, a static public IP and certified HIP service.

5. **Maintain OPD and IPD records digitally for the long term** – As per EHR Standards 2016, all electronic medical records must compulsorily be preserved and never destroyed during the lifetime of the person. The HIP / HRP is expected to store digital formats of the health records as per these guidelines. For diagnostic images like CT Scans / MRIs which are very large, storage of the full resolution images (preferably in DICOM formats) is required for a reasonable period that would allow the patient to download such files and store a copy in their Health Locker which is their personal storage. For these diagnostic reports, the HIP / HRP is expected to store the radiologist opinion and sample images that are normally part of the printed report provided to the patient. Any health records maintained by the HIP needs to be stored and managed securely in accordance with NDHM Health Data Management Policy and Information Security Policy for external ecosystem

6. **Share aggregated data for public health** – Every HIP service also generates a data feed with information that will be useful for public health purposes. This could include details like patients treated, count of treatments provided, number of tests conducted etc. Data from these services will be aggregated in a federated health analytics platform at the state and central levels. Except wherever specifically authorized by law, no individual HIP level data will be available to any entity, including the Government, so as to maintain privacy / confidentiality of a HIP's services.

7. **Migrate Health data on change of status -** Healthcare facilities (HIPs) could shut down services, move locations, change their HRP, etc. These scenarios can impact the HIP service and availability of Health data for their patients. HIPs commit to properly migrate data to an alternate provider in such scenarios. The detailed policies for the same will be worked out in consultation with the industry.

3.2 Issuing Health IDs to interested users

Any patient/ person who wishes to obtain a digital copy of their health records must first obtain a Health ID. The process is completely voluntary. Patients decide if they want to have Health ID and also decide when to share it with a healthcare provider. Health IDs can be created by either self-registration or in an assisted manner at a healthcare provider or other authorized entities. HIPs are expected to educate patients on obtaining a Health ID to access their health records digitally.

1. **Self-Registration** -- Health IDs can be created by providing a minimum set of information which include Full Name, Year of Birth, Gender and either a Mobile or an Aadhaar number. Most patients/ persons with smartphones are expected to self-enroll for the creation of a Health ID by downloading a PHR (Personal Health Record) mobile application or on the official Health ID portal (https://healthid.ndhm.gov.in).

2. **Assisted Registration** – Healthcare providers can assist patients in creating Health IDs. This is especially required in the case of the elderly, digitally illiterate and those without mobile phones. Every Health ID must be created only after educating the patient regarding the benefits of the Health ID and obtaining a clear consent of the patient. Healthcare facilities can either create the Health ID for patients from the official Health ID portal (http://healthid.ndhm.gov.in) or by integrating with the Health ID Open APIs from their own software. Details on setting up a Health ID desk is available in the NDHM Sandbox website. All patients obtaining Health IDs via an assisted mode must also receive a printed physical card containing the Health ID number and the QR code from the Health ID service. The Health ID service provides a standard card format that can be printed, folded and put into a plastic pouch or laminated. Users must be educated and encouraged to produce their Health ID at every Healthcare provider.

3. **Health ID and existing health provider cards** – Many health providers already issue patient identifier cards containing a provider specific patient id. These providers are encouraged to update their processes to include the Health ID No and the Health ID QR code on their existing cards. This can be achieved by integrating with the Health ID Open APIs in their software.

4. **Health ID and Children** – Newborns and infants must be issued Health IDs. These Health IDs must be linked to a nominee – usually a parent or guardian. By creating Health Ids for newborns HIPs can ensure that vital Health information right from their birth including immunization records becomes part of the child's longitudinal health record.

5. **Users who do not want Health IDs** –One of the guiding principles of NDHM is to put the patient in control of their health data. There are many scenarios where a patient may not want to create a Health ID or provide a Health ID to a care provider. HIPs are expected to follow their normal process of patient registration and care if a patient does not want a Health ID. HIPs are encouraged to minimally capture Name, Year of Birth, Gender and Mobile numbers for all patients.

3.3 Notifications and Linking of Health Records

Every Health ID in the NDHM ecosystem is linked to a health data consent manager. Health IDs and Health ID numbers are represented like *ashokb@ndhm* where @ndhm represents the health data consent manager. NDHM expects there to be multiple consent managers in the ecosystem over time.

The consent manager maintains information on which HIPs have health records for each Health ID. HIPs link a care context for each health encounter of the patient with the consent manager. Each care

context can contain multiple health records like diagnostic reports, discharge summaries, prescriptions, etc.

1. HIPs are encouraged to share a **digital** copy of any report that they share as a **printed and/or written** report with patients. This includes diagnostic reports, discharge summaries, OPD notes, prescriptions, etc.

2. If the HIP has collected and verified a Health ID from the patient, the HIP must use the HIP initiated linking method to link the care context with the associated health data consent manager. The consent manager will notify the patient that a new health record is available and allow the patients to access the same on their mobile or save a copy into their Health Locker.

3. If the HIP does not have a verified Health ID, but has captured the mobile number of the patient during registration, the HIP must send a SMS containing a deep link to the patient. The content of the SMS should educate the patient that they can access their health records from the healthcare provider. NDHM will specify the deep link to point to a category of PHR applications. The patient will be able to select and download any PHR application of their choice from the marketplace.

3.4 Format of health records to be shared

NDHM will define the Health data interchange standards to be used to ensure that data shared by HIPs can be correctly presented by HIUs. NDHM's approach is to ensure that data can be shared in both human readable and machine-readable formats while it works with the ecosystem for stronger adoption of eHealth standards. The current version of the health data interchange standards supports sharing of information in one of the following ways:

- Simple text based format
- Simple structure with attachments like PDF, JPEG, MPEG etc.
- Fully structured format with use of standard terminology code sets like SNOMED-CT, LOINC, ICD-11 etc.

The following guidelines have been adopted for the design of the Health data exchange specifications

1. All health records will use FHIR R4 resource bundles that have been profiled for the Indian context in collaboration with National Resource Centre for EHR Standards. These have been published at (https://www.nrces.in/ndhm)

2. The Health data interchange standards v1.0 covers the following document types
   a) **Diagnostic reports** – Formats are available for both pathology and radiology reports. While the format allows for existing PDFs / Images to be attached, we encourage HIPs to move to a strongly coded format over time. Full DICOM images (Imaging studies) are not yet supported and will be released in the next version
   b) **Discharge summary** – For recording of the final discharge summary for all inpatients

c) **Prescriptions** – The OPD prescription or Discharge Prescription can be shared in a semi-structured format with adoption of SNOMED-CT to capture the medication names. There is an option to attach a PDF version of the prescription as well.

d) OPD Consultation Note – The consultation note given to a patient at the end of the OPD encounter. The health data interchange standard provides a semi-structured, free text version and attachment options for sharing this document.

Additional document types and resources including immunization records will be released shortly**.** If there are specific types of documents that are currently not covered or areas that require more attention, please write to the NDHM team. Contact details are available at https://sandbox.ndhm.gov.in

4 Health Repository Provider Guidelines

Health repository providers are software service providers who offer NDHM compliant software and long-term storage of health records to HIPs. HRPs are required to fully comply with all guidelines specified for HIPs. Their primary role is to enable HIPs to meet their obligations of sharing and securely maintaining health records of patients digitally. For example, a hosted lab information management system provider (LIMS) may update their software to become a NDHM compatible Health Repository Provider. Any lab using this LIMS software can rapidly become a HIP by adopting the software.

a) The upcoming personal data protection bill (PDP Bill 2019) outlines a data fiduciary role to anyone creating personal data. All Healthcare providers will be data fiduciaries as they create personal health data. Health repository providers will help healthcare providers to meet the data fiduciary obligations under the personal data protection bill.

b) Health repository providers must provide long term storage of health records and high availability of the HIP service.

c) Large healthcare providers and public health programs play both the role of HIP and HRP. For example the e-Hospital software from NIC would enable one or more district hospitals and also maintain all the health records created at the hospital for several years. The RCH program would maintain the immunization records of children as a HIP / HRP for several years.

d) HIPs / HRPs are expected to store digital records of healthcare interventions including **outpatient** and **inpatient** treatments in a long-term storage and make them accessible to the health information provider service. HRPs are expected to use storage optimization techniques that provide high efficiency. Large format files like CT Scans / MRIs are expected to be available for a reasonable period allowing individuals to download and store the records. Users are expected to download and save in their own private Health Lockers. For these diagnostic reports the HIP / HRP is expected to store the radiologist opinion and sample images that are normally part of the printed report provided to the patient for long term.

e) There will be several scenarios when a HIP / HRP may not be able to continue to keep health data for patients, for example when they decide to stop providing health services. HRPs will need to ensure they comply with NDHM data migration guidelines to ensure there is no impact for patients.

f) HRPs must register with NDHM and obtain access keys for access to the NDHM network.

5 Health Information User Guidelines

Any entity that would like to access health records of a patient is called a Health Information User. This would include hospitals / doctors who would like to view medical history of patients, mobile applications or portals that want to display health data to patients including Personal Health Record applications, etc.

1. Any entity that wants to become an HIU will need to register with NDHM and obtain the access key.

2. No records will be accessible to HIUs without the consent of the patient. Consents in NDHM are based on the MeitY consent framework http://dla.gov.in/sites/default/files/pdf/MeitY-Consent-Tech-Framework%20v1.1.pdf. A digital consent artefact defining the purpose of use, the duration for which data will be available and document to the HIU is created each time the health records are shared.

3. Any health data that is held by an HIU is bound by the data rules set in the consent artefact provided along with the data. The data section of the consent artefact provides for view or copy rights including the period for which the data can be retained by the HIU.

4. Consents can be revoked. Patients may revoke access to information at any point they desire. HIUs implementations will require certification to ensure they adhere to the rules of the consent artefact.

5. Smart phone users can provide and manage consents from their smartphone PHR app

6. Aadhaar Health ID users can provide consent via their biometric auth at the HIU to allow access to their health data.

7. HIUs need to correctly handle variations of the health record formats as per the NHDM Health Data interchange specifications. The specifications allow simple PDF documents / images to fully structured and coded health data to be shared. The specifications are published at https://www.nrces.in/ndhm

8. Any health records obtained by the HIU needs to be stored and managed securely in accordance with NDHM Health Data Management policy and Information Security Policy for external ecosystem

6 Health Locker Guidelines

Health Lockers are software service providers who offer long term storage of records to individuals. Health Lockers behave like HIUs when they are receiving health records of the user from healthcare providers. Health Lockers behave like an HIP when the individual shares his records from his Health Locker. Apart from Health records from recognized healthcare providers, Health Lockers also can store user uploaded health records.

While Health Lockers behave like HIUs and HIPs not all guidelines of HIU/HIPs would be applicable on Health Lockers. Health Lockers need to implement the following guidelines.

1. Any entity that wants to become an Health Locker will need to register with NDHM and obtain the access key.

2. Health Lockers need to obtain a consent artefact from the individual that allows the locker to obtain and store all Health records of the individual forever.

3. Any health records in the Health Locker needs to be stored and managed securely in accordance with NDHM Health Data Management policy and Information Security Policy for external ecosystem

4. Health Lockers may also preferably implement the HIP service to allow sharing of records with appropriate user consent. The guidelines related to the HIP service including support for standards and uptime of services must be followed.

7 NDHM Sandbox for HIP and HIUs

The NDHM sandbox is the starting point for software developers who wish to ensure their healthcare software is compliant to the HIP, HRP, HIU and Health Locker guidelines.

1. Access to the Sandbox and its APIs is open to everyone under the NDHM Sandbox policy. Just sign up at https://sandbox.ndhm.gov.in to obtain access

2. The Sandbox hosts of the following digital building blocks
    a) Health ID Service and APIs – Create a sandbox Health ID, integrate your software with the Health ID APIs
    b) Consent Manager and Gateway – Register your software as a HIP, HRP, HIU or Health Locker and ensure you are able to correctly link records, process consent requests
    c) Sandbox PHR Mobile Application for Android – Use the application to manage your Health ID, view health records and manage consents
    d) Sandbox HIU application to create consent requests for a Health ID
    e) Sandbox DigiDoctor and APIs to register and verify doctors
    f) Sandbox Health Facility Registry and APIs to register and verify facilities

3. Documentation will be available on all the Open APIs hosted in the SandBox

4. Discussion forum where the NDHM team will answer tech queries and support implementers in the process.

5. NDHM test harnesses that will allow developers to check their implementation against the Open APIs

6. Once a software system has been integrated and tested in the SandBox, it can apply for NDHM compliance certification. NDHM will notify the agencies who are empaneled to certify the software as compliant to NDHM requirements. This is required to ensure correct capture and linking of health ids, secure storage of health data, use of standards in data exchange, etc

7. Access keys to NDHM production systems will be issued only post verification of the entity in the NDHM Registry and software being certified. This ensures only valid healthcare facilities and compliant software can participate in the NDHM ecosystem