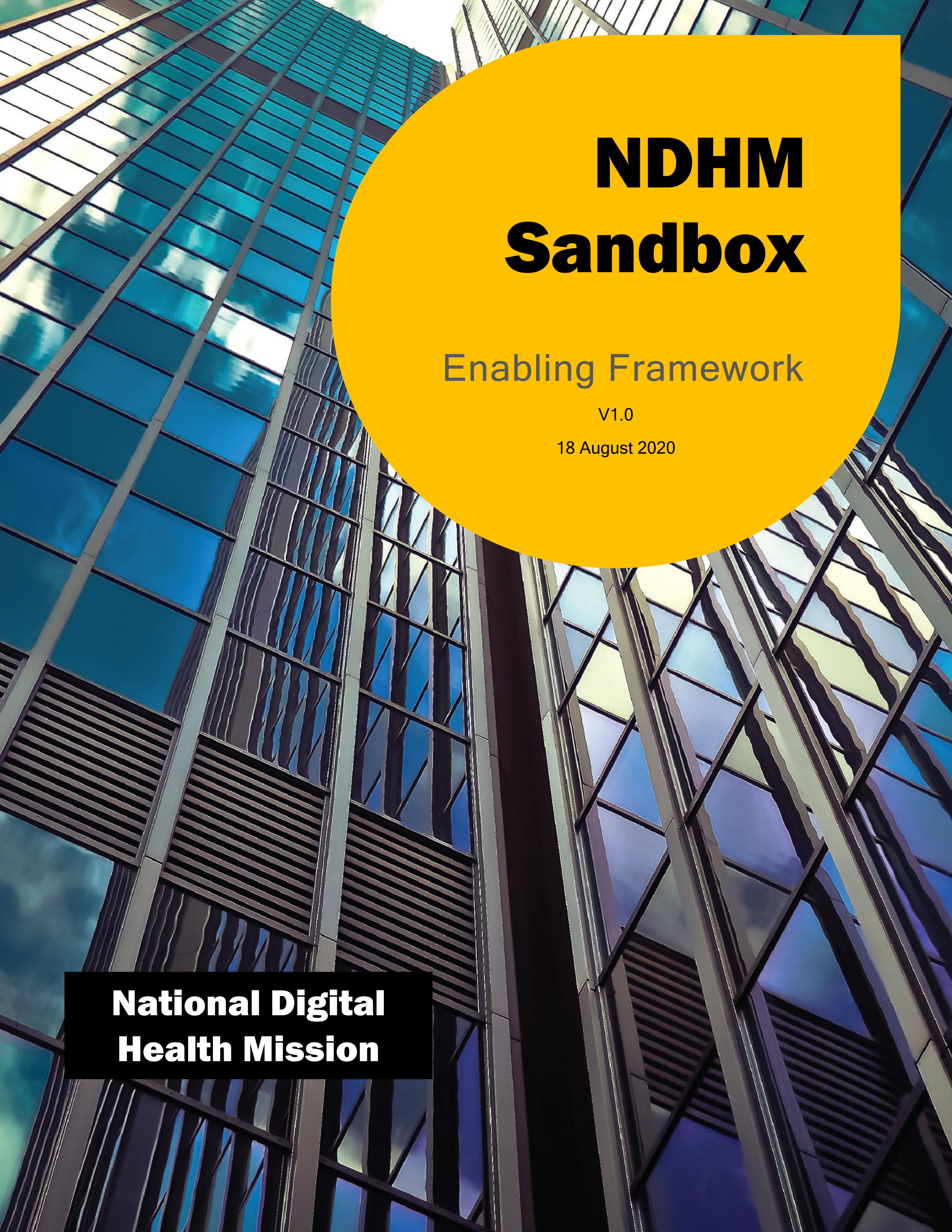


NDHM Sandbox

Enabling Framework

V1.0

18 August 2020

National Digital Health Mission

GLOSSARY

CDS	Clinical Decision Support
CIA	Confidentiality, Integrity, Availability
EMR	Electronic Medical Record
HIP	Health Information Provider
HIU	Health Information User
HTC	Health Tech Committee
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IT	Information Technology
KYC	Know Your Customer
LLP	Limited Liability Partnership
NDHE	National Digital Health Ecosystem
NDHM	National Digital Health Mission
NHA	National Health Authority
NS	National Digital Health Mission Sandbox
PDP	Personal Data Protection
PHR	Personal Health Record
SSH	Secure Shell
SSL	Secure Socket Layer
STQC	Standardization Testing and Quality Certification
VPN	Virtual Private Network

NDHM Sandbox

NDHM Sandbox is a framework that will allow technologies or products to be tested in the contained environment in compliance with NDHM standards and judge the consumer and market reactions to the same. This will help organizations intending to be a part of the National Digital Health Ecosystem to become a Health Information Provider or Health Information User or efficiently link with building blocks of NDHM.

Because there are boundary conditions - the risk is minimized and the emphasis is on feedback, learning and compliance to defined standards required to become a part of NDHM. This will provide an opportunity to "identify, understand, adapt, and respond to these disruptive new products and services" in a timely and appropriate fashion.

The environment will allow for both alpha as well as beta testing of the products, and accesses to NDHM ecosystem shall be primarily through the sandbox.

01

Be a part of the journey to create National Digital Health Ecosystem

02

Build products and components integrating with Building Blocks of National Digital Health Mission

03

Leverage the components using open standards and open APIs to expand your products; give choice to individuals on their choice of healthcare, promoting inclusivity

How does the sandbox work?

Subject to these guidelines and other guidelines and rules of Government of India, the sandbox access is open to all upon request. If your request is approved, you will get an access to the sandbox to build or/and expand your products in the healthcare / health tech industry. This is your chance to partner with NDHM, by enabling and empowering the products with the core building blocks of the Mission. For Government sector as well, APIs and platforms shall be available for integration with NDHM ecosystem.

Why should you partner?

The National Digital Health Mission is creating the core building blocks of healthcare. These building blocks include:

Health ID - a health identifier to every individual

DigiDoctor - a unique identifier to every doctor of every stream of medicine in the country and have his/her qualification/ occupation/ certification updated

Health Facility Registry - enabling all health facilities like hospitals, clinics, labs, pharmacies to have a unique identifier and have standardized single point of updated information PHR system - that gives a choice to every individual to have their personal health records under their control.

Thus, NDHM is creating building blocks enabling a highly efficient and effective healthcare experience and promoting inclusivity - taking healthcare to every corner of the country.

The Sandbox allows you to utilize the services and build products that shall contribute to the betterment of healthcare in the country.

It paves the way for an institution/system to become a Health Information Provider or a Health Information User utilizing the NDHM technologies.

Where to go to apply and be a part of NDHM Sandbox?
Apply online. Go to https://ndhm.gov.in for more details.

1. Background

1.1. The Ministry of Health and Family Welfare has conceived the idea of the National Digital Health Mission (NDHM). This visionary initiative of the Government of India, stemming from the National Health Policy, 2017 intends to digitize healthcare in India. This would be done by creating digital health records and creating and maintaining registries for healthcare professionals and health facilities, to ensure a smooth, interoperable framework for the multiple stakeholders in the healthcare ecosystem in India.

1.2. The National Digital Health Blueprint, 2019 recommends that a federated architecture be adopted, instead of a centralized architecture for the management of health data to ensure interoperability, technological flexibility, and independence across the National Digital Health Ecosystem (NDHE). The data collected across NDHE will be stored at three levels, i.e. at a Central level, at a State or Union Territory level and lastly, at the health facility level, adopting the principle of minimality at each level. The federated structure necessitates the development of a framework that can be utilized throughout the NDHE by public as well as private players to safeguard the privacy of individuals and confidentiality of health data that has been collected from individuals in India. This would be essential to build a trust quotient across the NDHE as well as to ensure that the personal and health data of all individuals in India is adequately protected, across the set of applications, platforms and systems that are a part of the ecosystem.

1.3. It will act as a guidance document across the NDHE and will set out the compliance, technical integrations, testing, scalability and minimum standard for data privacy protection that should be followed across the board in order to ensure compliance with relevant and applicable technological and healthcare standards, laws, rules and regulations.

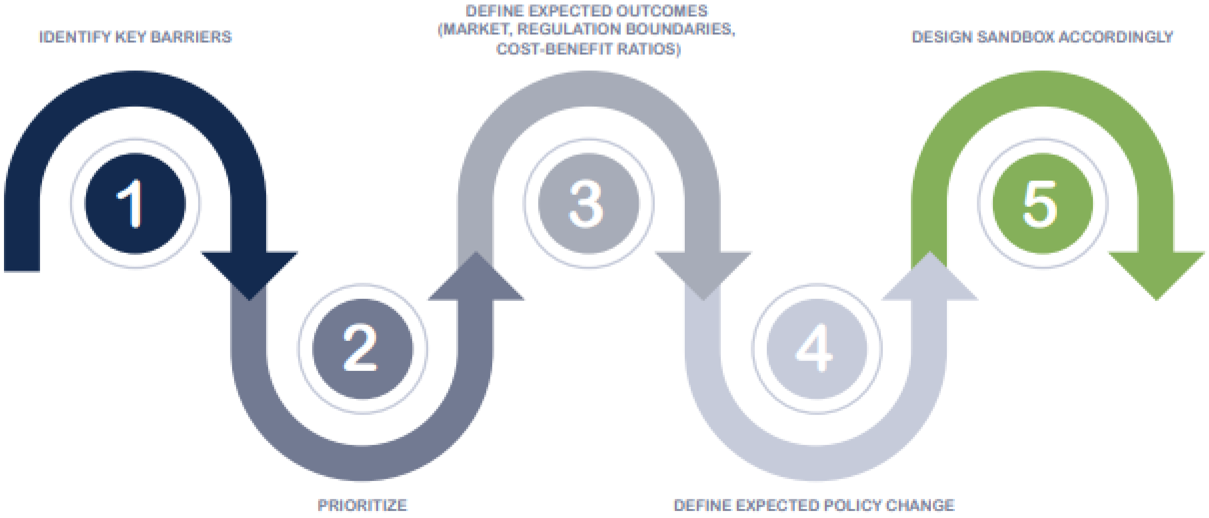
1.4. The NDHM Sandbox usage is not to be interpreted or construed as giving any entity or individual rights which are greater than those that such entity or individual would be entitled to under applicable laws. NDHM will investigate and report on the granular aspects of health tech and its implications to review the framework and respond to the dynamics of the rapidly evolving health tech scenario. The Mission is introducing an appropriate framework for a NDHM Sandbox (NS) within a well-defined space and duration where the health sector will come onboard to increase efficiency, manage risks, and create new opportunities for consumers.

1.5. Accordingly, a structure highlighting the clear principles and role of the proposed NS including the reasons for setting up the NS and the expectations of the NDHM, are detailed hereunder.

2. The NDHM Sandbox: Principles and Objectives

2.1. The NDHM Sandbox: NS for NDHM refers to live testing of the core building blocks and components of the Mission, and integrating them with new products or services in a controlled environment for which the NDHM shall provide access limited purpose of the testing. The NS will allow the Mission, the innovators, the healthcare service providers (as potential deployers of the technology) and the customers (as final users) to conduct alpha/beta/field tests of products integrated with NDHM building blocks and new healthcare/health tech innovations, while carefully monitoring and containing their risks. It can provide a structured avenue for the Mission to engage with partners and to develop innovation-enabling or innovation-responsive delivery of relevant health tech products. The NS is an important tool which will enable more dynamic, evidence-based systems which learn from, and evolve with, emerging technologies.

2.2. Objectives: The objective of the NS is to foster integration of current systems and IT platforms in healthcare to be integrated with NDHM building blocks, and also enable responsible innovation in health tech services, promote efficiency and bring benefit to consumers. The NS is, at its core, a formal programme for market participants to come forward to partner and integrate their current and new products, , services, or business models with customers in a near-live environment, subject to certain safeguards and oversight. The proposed health tech service to be launched under the NS should include the building blocks of NDHM mandatorily with new or emerging technology or use of existing technology in an innovative way and bring benefits to consumers.


IDENTIFY KEY BARRIERS
DEFINE EXPECTED OUTCOMES (MARKET, REGULATION BOUNDARIES, COST-BENEFIT RATIOS)
DESIGN SANDBOX ACCORDINGLY
1
2
3
4
5
PRIORITIZE
DEFINE EXPECTED POLICY CHANGE

3. NDHM Sandbox: Benefits

The setting up of an NS can bring several benefits, some of which are significant and are delineated below:

3.1. First and foremost, the NS fosters ‘learning by doing’ on all sides. The Mission will obtain first-hand empirical evidence on the benefits and risks of emerging technologies and their implications, enabling to take a considered view on supporting useful innovation, while containing the attendant risks. Incumbent healthcare / health tech service providers, including public health programs at centre and States, software providers, hospitals, labs, healthcare aggregators, and health tech companies and so on , also improve their understanding of how new healthcare / health tech technologies along with NDHM building blocks might work, which helps them to appropriately integrate such new technologies with their implementation / business plans.

3.2. Second, users of an NS can test the product's viability without the need for a larger and more expensive roll-out, if the product appears to have the potential to be successful. If any concerns arise, during the sandbox period, appropriate modifications can be made before the product is launched in the broader market.

3.3. Third, healthcare / health tech organizations provide solutions that can further inclusion and utilization of the NDHM in a significant way. The NS will go a long way in not only improving the pace of innovation and technology absorption but also in healthcare and health tech inclusion and in improving healthcare outreach.

3.4. Fourth, the NS will lead to better outcomes for consumers through an increased range of products and services, reduced costs, and improved access to healthcare services.

3.5. Finally, the NS will help developers and technical community of NDHM to get a first-hand feel of specifications, tools, technologies and building block of NDHM. It will provide an opportunity to the community to test their ideas and concepts and allow experimentation.

3.6. The data sharing shall be allowed based on approved Health Data Management Policy, Information Security Policy and any other policies as notified and applicable, and Data Protection Bill.

4. NDHM Sandbox: Risks and Limitations

4.1. The NDHM or its sandbox cannot provide any legal waivers.

4.2. Post-sandbox testing, a successful experimenter may still require necessary approvals before the product/services/technology can be permitted for wider application.

4.3. There is potential for some legal issues coming up, such as those relating to consumer losses in case of failed experimentation. Such instances may not have much legal ground if the NS framework and processes are transparent and have clear entry and exit criteria. Upfront clarity that liability for customer or business risks shall devolve on the entity entering the NS will be important in this context.

5. NDHM Sandbox: Eligibility Criteria

5.1. The target applicants for entry to the NS, are healthcare / health tech service providers, including public health programs at centre and States, software providers, hospitals, labs, healthcare aggregators, and health tech companies and so on and any other company partnering with or providing support to healthcare / health tech services businesses, subject to the sandbox criteria laid down in these guidelines. The focus of the NS will be to encourage innovations intended for use in the Indian market in areas where proposed innovation shows promise of easing/effecting delivery of healthcare / health tech services in a significant way.

6. Design Aspects of the NDHM Sandbox

The NDHM shall consider the following key design features for the NS:

6.1. NDHM Sandbox and Product/Services/Technology: The NS shall run an end-to-end sandbox process testing the products added to the sandbox during a defined period. The NS shall be based on adoption of NDHM, healthcare / health tech inclusion with NDHM building blocks, promotion, and usage of NDHM in an expansive manner, etc. The utilization of sandbox for different products may run for varying time periods as finalized by Health Tech Committee (HTC) under NDHM but should ordinarily be completed within six months. An indicative list of products/services/technology which could be considered for testing under NS is given below:

6.1.1. Products/Services

- Utilization of
  - Health ID
  - DigiDoctor Registry
  - Health Facility Registry
  - Personal Health Records
  - Telemedicine and Teleconsultation
  - e-Pharmacy
  - Health Clouds
- Convergence and expansion of NDHM for
  - Retail healthcare
  - Health Insurance and Health Assurance services
  - Healthcare Marketplace and aggregation
  - Digital KYC for healthcare
  - Healthcare / Health tech advisory services
  - Health management services
  - Digital health related identification services
  - Smart contracts
  - Healthcare inclusion products
  - Cyber security products
- Products like Clinical Decision Support System (CDS), Research- Medical & Policy, Anonymization-as-a-service, Consent Management as-a-service.

6.1.2. Technology

- Mobile technology applications
- Data Analytics
- Application Program Interface (APIs) services
- Applications under block chain technologies
- Artificial Intelligence and Machine Learning applications

6.1.3. Becoming a

- Health Information Provider (HIP): Any healthcare provider who creates health information in the context of treating a patient and agrees to share the same digitally with the patient using the consent framework adopted by the National Digital Health Mission (NDHM) is called a health information provider (HIP). Any Hospital, diagnostic centre, clinic, etc. will be able to become HIP by

  - Signing up with the NDHM facility registry to confirm they are a healthcare provider
  - Adopting EMR software that is certified to be compliant with NDHM standards.
  - The HIP should adopt identifiers maintained by NDHM (Health ID, DigiDoctor etc.)
  - The HIP must share anonymized data as per policy laid down by NDHM/NHA in this regard.

- Health Information User (HIU): Any entity that would like to access health records of a user will be called Health Information Users. This would include hospitals / doctors who would like to access medical history of patients, mobile applications that want to display health data to users including Personal Health Record applications. No record will be accessible to HIUs without the consent of the user.
- Health Repository Providers: HIPs are expected to store digital records of both outpatient and inpatient treatments in a long-term storage and make them accessible by the health information provider service. For HIPs that do not have the infrastructure in house, they are expected to partner with Health Repository Providers who will help them in implementing this obligation. This shall also cover health lockers and health data storage facility systems. These may act as Health Information Providers as well as Health Information Users.

Detailed guidelines for an organization to become HIP/HIU/Health Repository Provider shall be separately issued.

6.2. Quality Principles: The NS will need the following requirements to be mandatorily complied with by the applicants:

i. Customer privacy and data protection
ii. Secure storage of and access to data of all stakeholders, including health data
iii. Compliance to PDP 2019: The domain as well as technology/security audit is a mandatory component of getting an organization onboarded and going live with the NDHM ecosystem. The check on all compliances shall be a part of the audit.
iv. Compliance to medico-legal rules, regulations, and guidelines
v. Security of transactions
vi. NDHM core principles and related requirements
vii. Statutory restrictions
viii. Rules and regulations as finalized by MoHFW and MeitY

6.3. Exclusion from Sandbox Testing: Any product/services/companies/organizations which have been banned by the Government of India shall be strictly prohibited.

6.4. Fit and Proper Criteria for Selection of Participants in NS

6.4.1. Every applicant shall satisfy the following conditions:

a) It should either be a company/ proprietorship firm/ LLP/ firm/ institution/ organization incorporated and registered in India or licensed to operate in India. Further, healthcare / health tech institutions constituted under a statute in India would also be eligible.

b) The entity must demonstrate arrangements to ensure compliance with the existing regulations/laws on consumer data protection and privacy as well as PDP 2019.

c) There should be adequate safeguards built in its IT systems to ensure that it is protected against unauthorized access, alteration, destruction, disclosure or dissemination of records and data.

d) The test scenarios and expected outcomes of the NS experimentation should be clearly defined, and the sandbox entity should report to the Mission on the test progress, based on proposed schedule.

e) The appropriate boundary conditions (refer to section 6.7) should be clearly defined for the NS to be meaningfully executed while sufficiently protecting consumers' privacy.

f) An acceptable exit and transition strategy should be clearly defined in the event, that the proposed healthcare / health tech-driven service must be discontinued or can proceed to be deployed on a broader scale after exiting the NS.

g) The applicants shall be required to share the results of Proof of Concept (PoC)/testing of use cases including any relevant prior experiences before getting admission into NS for testing, wherever applicable.

h) Significant risks arising from the proposed healthcare / health tech solution or service should be assessed and mitigation plan shall be submitted.

6.4.2. The NS is an initiative to foster onboarding with NDHM, and responsible innovation in healthcare / health tech services, while carefully monitoring and containing their risks.

6.5. Extending or Exiting the NS

6.5.1. At the end of the sandbox period, the sandbox entity must exit the NS. In the event, that the sandbox entity requires an extension of the sandbox period, it should apply to the Mission at least one month before the expiration thereof and with valid reasons to support the application for extension. The Mission shall take an informed decision to allow extension or otherwise based on the stage of the testing, the results of the testing till then, justification for its continuance and the expected outcome in the extended period.

6.5.2. The sandbox testing will be discontinued any time at the discretion of the Mission:

a) if the sandbox entity does not achieve its intended purpose, based on the latest test scenarios, expected outcomes and schedule mutually agreed by the sandbox entity with the Mission.

b) if the sandbox entity is unable to fully comply with the relevant requirements and other conditions specified at any stage during the sandbox process.

c) if the sandbox entity has not acted in the best interest of consumers due to negligence or deliberate malicious practices

6.5.3. The sandbox entity may also exit from the NS at its own discretion by informing the Mission one month in advance. The sandbox entity shall ensure that any existing obligation to its customers of the healthcare / health tech service under experimentation is fully addressed before exiting the NS or discontinuing the NS.

6.6. Boundary Conditions: When the NS operates in the production environment, it must have a well-defined space and duration for the proposed healthcare / health tech service to be launched, within which the consequences of failure can be contained. The appropriate boundary conditions should be clearly defined for the NS to be meaningfully executed while sufficiently protecting the interests of consumers. The boundary conditions for the NS may include the following:

6.6.1. Start and end date of the NS

6.6.2. Target customer type

6.6.3. Limit on the number of customers involved if any

6.6.4. Security and privacy of data related conditions

6.6.5. Compliance to standards and processes for each building block of NDHM

6.7. Consumer Protection

Sandbox will require the applicant to present a plan which adequately protects its consumers. This may include marketplace disclosures, a risk management plan, safeguarding procedures, incident reporting and dispute resolution, redress mechanisms, or insurance (such as a fund for victim compensation). In addition, the applicant should have a plan with key milestones identifying key performance indicators to plot the trajectory on whether key objectives were met and associated learnings.

6.7.1. The sandbox entity will be required to ensure that any existing obligations to the customers of the healthcare / health tech service under experimentation are fulfilled or addressed before exiting or discontinuing the NS. It may be noted that entering the NS does not limit the sandbox entity’s liability towards its customers.

6.7.2. The entities entering the NS must, in an upfront and transparent way, notify test customers of potential risks and the available compensation and obtain their explicit consent in this regard. There should be an appropriate arrangement for customers to withdraw from the test.

6.7.3. Sandbox entities shall be required to take liability/indemnity insurance of an adequate amount and period to safeguard the interest of the customers. The adequacy of indemnity cover shall depend on determination of the maximum liability based on, among others, (i) maximum exposure to a single customer (ii) the number of claims that could arise from a single event (potential for multiple claims); and (iii) number of claims that might be expected during the policy period. The policy cover shall begin with the start of testing stage and end three months after exit of the sandbox entity from the NS.

6.8. For a Participant, which is a regulated entity operating in India under a license, the terms and conditions of that license would continue to apply during the test to all non-Sandbox approved activities. The Sandbox would permit a product, solution or service to be tested by the Mission in accordance with a test plan and without requiring a separate or modified license or authorization for the purposes of the test, once the Mission approves the application submitted by the participating entity and the security audit is successfully completed.

7. The NDHM Sandbox Process and its Stages

7.1. End-to-End Sandbox Process: A detailed end-to-end sandbox process, including the testing of the products/innovations by healthcare / health tech entities, shall be overseen by the NDHM Health Tech Committee (HTC) under overall guidance of the Mission Director, NDHM with participation of domain experts.

7.2. The Sandbox Process: Each product on NS shall have the following five stages and timeline:

7.2.1. Preliminary Screening: The application submission shall be always open and all applications shall be processed on FIFO basis. The applications shall be received by the HTC and evaluated to shortlist applicants meeting the eligibility criteria. The HTC shall ensure that the applicant clearly understands the objective and principles of the NS and conforms to them.

7.2.2. Test Design: This phase may last for 4 weeks. The HTC shall finalize the test design through an iterative engagement with the applicants and identify quantitative and/or qualitative outcome metrics for evaluating evidence of benefits and risks.

7.2.3. Application Assessment This phase may last for 3 weeks. The HTC shall vet the test design and propose modifications, if any.

7.2.4. Testing: This phase may last for a maximum of 12 weeks. The HTC shall assess by close monitoring.

7.2.5. Evaluation: This phase may last for 4 weeks. The outcome of the testing of products/services/technology as per the expected parameters including viability/ acceptability under the NS shall be confirmed by the NDHM. The HTC shall assess the outcome reports on the test and decide on whether the product/service is compliant with various NDHM guidelines.

8. Certification Process

8.1.1. With new global demands for Security and Quality, the need for software product assurance is becoming more important. There are essentially two approaches that can be followed to ensure product quality, one being assurance of the process by which the product is developed, and the other being the evaluation of the quality of the end-product. Both approaches are important, and both require the presence of a system for managing quality.

8.1.2. NDHM has engaged with Ministry of Electronics and Information Technology, Government of India to verify, validate and certify products/solutions who have onboarded with the NDHM Sandbox and shall be going live with the products, with mandatory integration of NDHM building blocks through APIs.

8.1.3. Standardization Testing and Quality Certification Directorate (STQC) shall be the organization responsible for ensuring the certification of the software/product with NDHM before it is rolled out in the open market. The certification/audit of the product shall be mandatory and shall be undertaken by STQC/empanelled vendors under STQC.

8.1.4. STQC offers testing for IT products and a variety of Software verification and Validation services. They are provided with well-trained manpower, state- of-the-art testing laboratories including software testing tools and office infrastructure. They act as a single point focus to provide third party validation services.

8.1.5. The following process shall be followed:

a) The organizations receiving clearance certificate from the HTC at NDHM shall reach out to STQC/empanelled vendor for certification/audit of the solution/product.

b) The STQC/empanelled vendor shall complete the audit within reasonable period from the date of receipt of access/credentials.

c) Once the audit report is shared by STQC/empanelled vendor, any changes asked for shall be done by the concerned organization and re-submit the solution/product for second level of audit.

d) If any functional/policy level issues are highlighted, or issues are highlighted which may have an impact on the components/building blocks of NDHM, STQC shall inform NDHM and it will be taken up by the HTC/product teams at NDHM.

e) The process as mentioned in point b and c as mentioned above shall be followed for each iteration of audit, till 5 iterations.

f) If a product does not clear the audit in 5 iterations, it will be deemed rejected, and a new application needs to be filed in each such case by the organization.

g) The cost of audit shall be borne by the organization. The maximum cost /ceiling shall be pre-defined, jointly finalized by MeitY and NDHM.

h) A certification/audit checklist shall be issued by STQC with the exact steps defined for the certifications/audits. The following is a non-exhaustive list of items that shall be checked during the audit:

1. The application/software/product has been placed in protected zones with implementation of firewalls and IDS (Intrusion Detection System) and high availability solutions.
2. Before launch of the application/software/product, simulated penetration tests have been conducted. Penetration testing has also been conducted <x times> after the launch of the application/software/product.
3. The application/software/product has been audited for known application level vulnerabilities before the launch and all the known vulnerability has been addressed.
4. Hardening (as and where needed) of servers has been done before the launch of the application/software/product.
5. Access to web servers hosting the application/software/product is restricted both physically and through the network as far as possible, the servers reside in India, and no data is shared out of India.
6. Logs at <x number> different locations are maintained for authorized physical access of application/software/product servers.
7. Web servers hosting the application/software/product are configured behind IDS, IPS (Intrusion Prevention System) and with system firewalls on them.
8. Encryption is enabled wherever required
9. Secure storage devices are utilized
10. Enablement of automatic wiping of lost or stolen devices
11. Secure Sockets Layer (SSL) in place when using the Internet to ensure secure data transfers
12. Secure email gateways ensuring data is emailed securely
13. All the development work is done on separate development environment and is well tested on staging server before updating it on the production server.
14. After testing properly on the staging server, the applications are uploaded to the production server using SSH and VPN through a single point.
15. The content contributed by/from remote locations is duly authenticated & is not published on the production server directly. Any content contributed to go through the moderation process before final publishing to the production server.
16. All contents/data of the pages are checked for intentional or unintentional malicious content before final upload to web server pages.
17. Audit and Log of all activities involving the operating system, access to the system, and access to applications are maintained and archived. All

rejected accesses and services are logged and listed in exception reports for further scrutiny.

18. Help Desk staff at the HTC monitor the application/software/ product at intervals of <frequency> to check the system to confirm that the application is up and running, that no unauthorized changes have been made, and that no unauthorized links have been established.
19. All newly released system software patches; bug fixes and upgrades are expeditiously and regularly reviewed and installed on the web/application server.
20. On Production servers, Internet browsing, mail and any other desktop applications are disabled. Only server administration related task is performed.
21. Server passwords are changed at the interval of <x number> months and are shared by <y number> persons <a name> and <b name>.
22. <a name> and <b name> have been designated as Administrator for the application/software/product and shall be responsible for implementing certification requirements for each of the servers. The administrator shall also coordinate with the Audit Team for required auditing of the server(s).
23. The application/software/ product has been re-audited for the application level vulnerability after major modification in application development [Not applicable at first launch].
24. CIA Model:
    1. **C**onfidentiality: Ensures that information is not accessible to unauthorized people—usually by enabling encryption—which is available in many forms.
    2. **I**ntegrity: Protects data and systems from being modified by unauthorized people; making sure that data has integrity and was not changed between the time you created it and the time it arrives at its intended party.
    3. **A**vailability: Ensures that authorized people can access the information when needed and that all hardware and software is maintained and updated when necessary.
25. Preventive security controls, designed to prevent cyber security incidents
26. Detective security controls, aimed at detecting a cyber security breach attempt (“event”) or successful breach (“incident”) while it is in progress, and alerting cyber security personnel
27. Corrective security controls, used after a cyber security incident to help minimize data loss and damage to the system or network, and restore critical business systems and processes as quickly as possible (“resilience”)

28. Technical controls such as multi-factor user authentication at login (login) and logical access controls, antivirus software, firewalls
29. Compliance controls such as privacy laws and cyber security frameworks and standards.

8.1.6. The Audit for the organizations participating in the sandbox shall be done as per the checklist finalized by NDHM.

9. Statutory and Legal Issues

9.1. Upon approval, the applicant becomes the sandbox entity responsible for operating in the NS. The NDHM will provide the appropriate support by relaxing specific requirements (which the sandbox entity will otherwise be subject to), where necessary, for the duration of the NS. The NDHM shall bear no liability arising from sandbox process and any liability arising from the experiment will be borne by the applicant as a sandbox entity.

9.2. Upon successful experimentation and on exiting the NS, the sandbox entity must fully comply with the relevant requirements. The applicant should clearly understand the objective and principles of the NS. It must be emphasized that the NS is not intended and cannot be used as means to circumvent legal and regulatory requirements.

9.3. At the end of the sandbox period, the sandbox entity must exit the NS, and start utilizing the production services of NDHM ecosystem to be continuing for live implementation.

10. Transparency and Disclosure

10.1. Outreach with stakeholders and clear and adequate information dissemination on the NS is important. The NDHM will communicate the entire sandbox process including its launch, successful applicants selected for NS, entry and exit criteria and products/services found viable and acceptable under the NS through its official website.

10.2. The NDHM shall reserve the right to publish any relevant information about the NS applicants on its website, including for the purpose of knowledge transfer and collaboration with other international agencies, without revealing any proprietary/intellectual property rights related information.