Information Security and Privacy under NDHM

National Digital Health Mission (NDHM) will promote and facilitate the evolution of the National Digital Health Ecosystem (NDHE) throughout the country as envisaged in the National Digital Health Blueprint (NDHB) which will result in a tremendous improvement in the efficiency, effectiveness, and transparency of the overall healthcare service delivery. Patients will be able to securely store and access their medical records (such as prescriptions, diagnostic reports, discharge summaries etc.), and share them with health care providers to ensure appropriate treatment and follow-up. Citizens will also have access to more accurate information on health facilities and providers. Further, they will have the option to use healthcare services remotely by using tele-medicine.

NDHM through its core application like registries, consent manager, Health ID, etc. will empower individuals with accurate information to enable informed decision making and enhance the accountability of the healthcare providers. NHA is fully seized of the fact that the flow of information being facilitated through NDHM is sensitive in nature.

Therefore, National Health Authority (NHA) acknowledges that institutionalization of an effective information security policy is a critical step in preventing security incidents and fostering a security conscious culture across National Digital Health Ecosystem (NDHE). The policies as mentioned below which are being implemented in NDHM are based on the principles outlined in National Digital Health Blueprint (NDHB).

1. NDHM Information Security Policy for Internal Ecosystem
2. NDHM Information Security Policy for External Ecosystem
3. NDHM Strategic Control Policy

1. **NDHM Information Security Policy for Internal Ecosystem**

This policy is applicable only to NDHM's internal ecosystem partners. It is designed to guide individual's behaviour with regard to the security of NDHM information and IT systems. This Policy document specifies safeguards to be deployed across NDHE for securing the critical digital infrastructure of our nation and for protecting the personal digital health data of all individuals

2. **NDHM Information Security Policy for External Ecosystem**

This Information Security Policy establishes the minimum benchmark to secure information assets of NDHM external ecosystem through a layered structure of overlapping controls and continuous monitoring. The policy serves as a central policy document with which all the Health Information Providers (HIPs), Health Information Users (HIUs) or any other ecosystem partner, must comply.

3. **NDHM Strategic Control Policy**

While the IT Infrastructure and applications of NDHM are established and maintained in contractual arrangements with the private sector players, the purpose of this policy is to retain complete control over the Strategic Assets of NDHM i.e. Software Applications, Databases, Network, Security, Storage and Core infrastructure of all the components of the mission like API gateway, Consent Manager, Personal Health Record (PHR) application and Health ID etc. in the ambit of NHA.

In an effort to ensure protection, security and privacy, and limit the distribution of this policy to only those with authorized access, these policies shall only be shared with concerned parties.