Ayushman Bharat Digital Mission

Guidelines for Creating ABHA (number) Using Digital Devices in Offline Mode

January 2022

1. **Introduction**
   ABDM has enabled the creation of Ayushman Bharat Health Account ("ABHA" (numbers)) for citizens of the country through self-registration and assisted mode. Realizing that there are geographical regions in the country where citizens do not have access or have limited access to internet/mobile connectivity, ABDM has provided an alternate way of creating the ABHA (number) using digital devices in offline mode to the willing citizens of the country. Adoption of ABDM will make healthcare services accessible, efficient, and affordable in these regions of the country.

2. **Purpose**
   The Purpose of these guidelines is to provide the minimum standards to be followed for creating ABHA (numbers) using digital devices in offline mode and ensuring compliance by the participating entities.

3. **Applicability**

   These guidelines shall be applicable to the "participating entity" like government health program, state government, central government, healthcare facility & center etc, which will facilitate the process of creating ABHA (numbers) in offline mode using digital devices for the beneficiaries through the assistance of "authorized personnel". The authorized personnel may include healthcare workers, officials from healthcare facilities, central government, state government, district administration and others.

   The provision to create ABHA (number) in offline mode will only be enabled for select government health programs, healthcare facilities & centers etc. The permission-based access will be provided by ABDM upon request. Also, this method of creating ABHA (number) is to be allowed only for geographical locations with no or limited internet/mobile connectivity.

   For the purpose of creating ABHA (number) using digital device in offline mode, the participating entity may use a program application developed by themselves or ABDM. The digital device to be used for the purpose of creating ABHA (number) may be a mobile, tablet or any other digital device approved by the participating entity.

4. **Sandbox integration of the program application**
   Any program application developed by the participating entity for the purpose of creating ABHA (number) using digital devices in offline mode shall undergo sandbox integration process of ABDM. The details regarding the sandbox process are available at https://sandbox.abdm.gov.in/.

5. **Criteria for allowing ABHA (number) creation in offline mode**
   ABDM shall allow creation of ABHA (numbers) under these guidelines at locations where there is no or limited internet /mobile connectivity.

6. **Collection of demographic information & consent**
    a. The authorized personnel are bound by these guidelines only when they are collecting the personal information of any individual only for the purpose of creation of ABHA (numbers). The authorized personnel shall not be bound to these guidelines if they are visiting the individuals for any purpose other than collecting data for creating ABHA (number).
    b. The authorized personnel shall explain the benefit of having ABHA (number) to the individuals and only once they are interested in applying for ABHA number, the authorized personnel shall request the individuals to show their Aadhar card. These benefits shall be explained either in English, Hindi or any other local language which individuals shall be able to understand.
    c. It is the duty of authorized personnel to verify and confirm the identity of the individual with the Aadhar card provided.
    d. The authorized personnel shall collect the requisite demographic information along with the Aadhar number from the Aadhar card of the interested individuals and will record the same correctly in program application on the device.
    e. The authorized personnel shall only collect requisite information from Aadhar card of individuals. Photocopies or images of Aadhar card shall not be collected under any circumstances.
    f. After recording the requisite information, the consent language is to be read out to the individual explaining all details in a language understood by him/her. If the individual agrees and provides his/her consent for processing his/her personal data for creating ABHA number, only then the authorized personnel shall capture the consent of the individual in the device and submit the information in the program application. If the individual does not agree for processing of his/her personal information for creating ABHA (number) after listening to the consent language, the application being filled must be cancelled at that time only.
    g. Once the requisite information for creating ABHA (number) along with the consent is recorded in the device, the safety and security of the device shall be the sole responsibility of the authorized personnel.

7. **Security & safety of collected data**
    a. It shall be the responsibility of the authorized personnel and the participating entity to ensure that the data collected & processed is safeguarded.
    b. Ensure adequate security training is provided to various end-users and security awareness programs are conducted regularly on collection, migration and disposal of the collected information.
    c. Processes must be in place to ensure data is destroyed or disposed upon the data retention period.
    d. Participating entities to comply with the Aadhar data vault requirement as per Aadhar circular 2.11
    e. Ensure appropriate evaluation, testing and audits of all structures, mechanisms, policies, procedures. Areas of improvement should be identified and a mechanism to improve the

overall deployment of such structures, mechanisms, policies, procedures, technologies and controls should be undertaken.

f. Ensure the minimum data is collected which will suffice the authentication of the personnel.

g. Ensure prior consent to be accorded before collection of the information.

h. The data collected to be stored in encrypted or any other secured format till the same is not synced with ABDM server. Implement a mechanism to encrypt, using AES 256-bitsymmetric encryption of personal data and digital health data at rest/transition. Encryption keys must be protected securely, preferably using Asymmetric cryptography/algorithm (PKI) RSA 2048.

8. Syncing & generation of ABHA (number)

a. The authorized personnel shall take the device to an office or center of participating entity or any other place with proper internet connectivity for further processing and syncing of the data with ABDM server.

b. Upon successful syncing of data with ABDM server, the ABHA (number) cards of the individuals will be created and be available in the program application on the device.

c. If the syncing of data with ABDM server is unsuccessful for any reasons beyond the control of authorized personnel, the ABHA card will not be created. In this case, these records pertaining to such individuals for whom the ABHA card has not been generated, have to be deleted by the authorized personnel. The authorized personnel will have to collect and record information from such individuals again along with a fresh consent.

d. The authorized personnel shall download the ABHA (number) cards generated after the successful syncing.

9. Deletion of records from the device

The deletion of records shall be an ongoing process and not a one-time exercise. The participating entity shall ensure the following -

a. The authorized personnel shall delete the records which were not successfully synced with ABDM server after every round of syncing.

b. The authorized personnel shall delete the ABHA cards generated after printing the same within 30 days of their generation.

c. Authorized Personnel to give a declaration on regular intervals confirming the deletion of ABHA (number) cards generated before 30 days from the date of declaration.

10. Communicating ABHA (number) to the beneficiary

a. ABHA system shall communicate the ABHA (number) generated to the beneficiary on his/her registered mobile number.

b. After downloading the ABHA cards generated post successful syncing of records with ABDM server, the authorized personnel shall print the ABHA cards of the beneficiary.

c. The authorized personnel shall deliver the printed ABHA cards to the beneficiaries within the reasonable time as decided by the participating entity.

d. Till the time ABHA cards are not delivered to the beneficiaries, the safety and security of printed ABHA cards shall be the sole responsibility of the authorized personnel.

11. Compliance

a. ABDM may enforce an audit of any office or center of entity participating in creating ABHA (numbers) in offline mode using digital devices.

b. The participating entity must undertake all reasonable security measures to protect the data of the individuals being collected and processed by them.

c. The participating entity shall ensure that they have an independent audit mechanism to do audits checks of the devices used by authorized personnel for data collection and storage.

d. Any privacy breach must be notified by the authorized personnel / participating entity to the individual concerned and the ABDM.

e. The participating entity shall ensure that the records belonging to more than 30 days old are deleted from the devices being used under these guidelines.