NACO
National AIDS Control Organisation
India's Voice against AIDS
Ministry of Health & Family Welfare, Government of India
www.naco.gov.in

Ministry of Health & Family Welfare
Government of India

आज़ादी का अमृत महोत्सव

Standard Operating Procedure for NACP Data Management at NACO, SACS and NACP establishment

1. Definitions with respect to NACP Data Management:

Head of Division: Senior most officer and in-charge of respective programme division at NACO and SACS.
I/C of NACP establishment: In-charge of NACP establishment.
SACS: It includes all State AIDS Control Societies and Mumbai Districts AIDS Control Society.
NACP establishment: It includes all establishments involved in prevention, testing, care, and treatment under the National AIDS Control Programme.
Organization authorized to share data: At national level, NACO and at state level, SACS.
Agencies under MoU/Other Government Department: Institutions involved in NACP related activities as per MoU with NACO/SACS and other government department at National and State level.
Outside NACP: Bilateral/ Implementing Partners/ Agencies without MoU/Individuals/Non-governments/Privates/Others.
National Data hub: Repository of all approved NACP data including data from research, surveillance, survey/ study conducted by NACO and SACS.
Custodian of Data: NACO and concerned SACS are the custodians.

2. Scope

This SOP applies to all personnel involved in handling of NACP data at NACO/SACS/NACP establishment level and those who seek data from NACO/SACS including TSU.

3. Goal

The main goal of this SOP is to streamline data management at NACO, SACS and at NACP establishment levels. This SOP will help to restrict unauthorized data access.

4. NACP data access at NACO, SACS and at the NACP establishment

Head of Division at NACO, SACS and I/C of NACP establishment will have access to NACP data available in Information Management System (IMS). Data Management and repository function will be looked after by HoD SI at NACO or SACS.

5. Composition of Data Management Committee (DMC)

DMC should be formed at each establishment. Concerned DMC is responsible to ensure data security and also to review and provide appropriate recommendation regarding data security measures. These data management committee will supersede all existing committees at NACO, SACS and establishment level. Wherever establishment does not have DMC, the head of the establishment should be entrusted with the responsibility and function of DMC. Details of composition as well roles and responsibility are given in below table:

Composition of DMC		
At NACO & SACS		**At NACP Establishment**
Chairperson	Senior most head of division	Senior and relevant officer of the establishment
Members	• Head of all Divisions • One subject expert as per need and approval of the chair	The committee will have 2 members, one of the members should be representatives from protected person and other from the same establishment who deals with the data
Member Secretary	HoD SI Division	
Terms of Reference		
At National Level	**At State Level**	**Establishment Level**
• To review data requests received at NACO.	• To review data requests received at SACS.	• Review of implementation of data protection measures at the establishment.

• To provide inputs on disposal of physical file/ computer equipment containing HIV related information at NACO. • To consider all adverse event related to NACP data reported to the committee. • Review of data access and data security at NACO and SACS. • Any other matter related to NACP data management.	• To provide inputs on disposal of physical file/ computer equipment containing HIV related information at SACS. • To consider all adverse event related to NACP data reported to the committee. • Review of data access and data security at SACS and NACP establishments within the state. • Any other matter related to NACP data management.	• Review of data access and data security at the establishment. • To provide inputs on disposal of physical file/ computer equipment containing HIV related information at the establishment. • To consider all adverse event related to NACP data reported to the committee. • Any other matter related to NACP data management.

6. Steps for data management at NACO, SACS and NACP establishment:
It is mandatory for every establishment that keeps the records of HIV-related information of protected persons to adopt data protection measures. Data protection measures here include following steps:

- **Protecting information from disclosure of HIV related information**: Confidentiality and privacy is to be maintained while collecting HIV-related information. For each establishment desirous of collecting the HIV related information, authorized persons or staff should sign an undertaking for data confidentiality.

- **Access to HIV-related information:** Access should be granted only to the authorized persons/ staff after they sign a formal undertaking for confidentiality.

- **Provision for security systems for HIV related information**:
  - ✓ There should be secured almirahs or cabinet for physical records like registers, reports etc. which should be carefully locked when not being used.
  - ✓ Establishments should ensure that computer systems having HIV related information are protected by using appropriate and up-to-date anti-virus and firewall technologies and it is to be kept up- to-date to meet emerging threats.
  - ✓ Personal computers or mobiles or tablets or any other hardware with HIV related information should be password protected and should be logged off or 'locked' when not being used.
  - ✓ Passwords for hardware, software, databases, etc. should be of sufficient strength. Establishments must also ensure that passwords are changed on a regular basis.
  - ✓ A Strong Password must
    - ▪ Be at least 8 characters in length
    - ▪ Contain both upper and lowercase alphabetic characters (e.g. A-Z, a-z)
    - ▪ Have at least one numerical character (e.g. 0-9)
    - ▪ Have at least one special character (e.g. ~!@#$%^&*()_-+=)
  - ✓ Any software or applications for maintaining the HIV-related information of protected persons in the establishment should be explicitly approved by competent authority of the respective institution.

- **Disposal of HIV related information:** Establishment should have standard operating procedures (SOPs) in place regarding the disposal of physical and electronic records/files containing HIV-related information of protected persons.

- **Accountability and liability** of security of HIV related information should be with Data Management Committees or the head of the concerned establishment where DMC is not constituted.

7. NACP data sharing through shared confidentiality: NACP data is only to be shared by NACO and SACS as per the SOP for NACP data sharing.

8. Monitoring:
Access to files/data containing HIV-related information of protected persons will be monitored by SI Division (Data Analysis & Use) at NACO and in-charge of SI Division at SACS on a regular basis.

Reference: The HIV and AIDS (Prevention & Control), Act 2017

For additional information, NACO's guidelines and official website may be referred to from time to time.