

T-11020/23/2020/NACO/SI-DATA  
Ministry of Health and Family Welfare  
National AIDS Control Organisation

6th & 9th Floor, Chanderlok Building  
36, Janpath, New Delhi – 110001  
Dated: 29-10-2020

**Subject: Draft NACP Data Management Guidelines 2020 under National AIDS Control Programme, Ministry of Health and Family Welfare – reg.**

Dear Sir/Madam,

As you may be aware, the Government of India has enacted HIV and AIDS Prevention and Control Act, 2017 for safeguarding the rights of People Living with HIV (PLHIV). One of the provisions of the Act is to adopt data protection measures in accordance with the guidelines to ensure that such information is protected from disclosure.

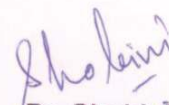
The National AIDS Control Programme (NACP) generates considerable data on HIV/AIDS from service facilities through the Management Information system, research projects, HIV Sentinel Surveillance etc. Hence there is a need to have a uniform mechanism for maintaining data security and also have checks and balances while providing access to this data to stakeholders and partners for programmatic and academic activities.

In this context, NACO had earlier developed Data Sharing Guidelines, 2018 for sharing of NACP Data and subsequently Data Protection Guidelines, 2019 was developed for protection of information of PLHIV in the context of HIV/AIDS (P&C) Act 2017 (both are available on <http://naco.gov.in/>). In order to align these two documents and to bring greater clarity on various aspects of Data Management, a comprehensive "NACP Data Management Guidelines, 2020" has been drafted.

The document has been seen by Ministry of Electronics & Information Technology (MeitY), Government of India and is aligned with the Draft Personal Data Protection Bill, 2019.

The draft document is being uploaded on the website of NACO to be used as an interim reference. The Standard Operating Protocols given in the guidelines may be referred to while submitting request for data sharing or any other related matters. In case there are inputs or comments on the draft guideline, they may be sent to the email id [data.naco@gmail.com](mailto:data.naco@gmail.com).

With best regards,



**Dr. Shobini Rajan**

Deputy Director General (SI)

Email: [shobini.simu.naco@gmail.com](mailto:shobini.simu.naco@gmail.com)

Tel: 23731810/ 43509956

*Enclosure: Draft NACP Data Management Guidelines, 2020*

**National AIDS Control Programme  
Data Management Guidelines  
2020**

**FOR DATA COLLECTION, PROTECTION AND SHARING**



---

**National AIDS Control Organisation**  
**India's Voice against AIDS**  
Ministry of Health & Family Welfare, Government of India  
[www.naco.gov.in](http://www.naco.gov.in)

## Contents

Executive Summary .....	3
1. Introduction.....	5
<b>1.1 Background</b> .....	5
<b>1.2 Scope and Evolution of data sharing and protection guidelines of NACO</b> .....	5
<b>1.3 Type of NACP Data</b> .....	6
<b>1.4 Data Capture Systems under NACP and Data flow</b> .....	7
<b>1.5 Data Availability</b> .....	7
2. Key Definition .....	8
3. NACP Data Storage and Protection .....	9
<b>3.1 Data Storage, Protection and Access</b> .....	9
<b>3.2 NACP Data Hub</b> .....	12
<b>3.3 Data Management Committee and Structure</b> .....	13
<b>3.4 Security level of NACP Data</b> .....	14
4. NACP Data Sharing and Transfer.....	15
<b>4.1 Data sharing and transfer cycle</b> .....	15
<b>4.2 Matrix of data approval and sharing</b> .....	16
<b>4.3 Data sharing process</b> .....	19
5. Data disposal at NACO/SACS/RU.....	20
6. Risk Mitigation/ Adverse events management.....	20
7. Data security monitoring at NACO, SACS and RUs.....	21
8. Role of Information Technology.....	221
Annexure –I .....	233
Annexure-II.....	28
Annexure-III .....	30
Annexure -IV .....	31
Annexure -V.....	32
Annexure –VI.....	33
Annexure –VII .....	34

## List of Abbreviations

AIDS	Acquired Immunodeficiency Syndrome
BSS	Behavioural Surveillance Survey
CMIS	Computerized Management Information System
DAPCU	District AIDS Prevention and Control Unit
DD	Deputy Director
DDG	Deputy Director General
HIV	Human Immunodeficiency Virus
HIV/AIDS Act, 2017	Human Immunodeficiency Virus (HIV) and Acquired Immune Deficiency Syndrome (AIDS) (Prevention and Control) Act, 2017
HoD	Head of Division
HSS	HIV Sentinel Surveillance
IBBS	Integrated Biological and Behavioural Surveillance
IMS	Integrated Management System
IT	Information Technology
NACO	National AIDS Control Organization
NACP	National AIDS Control Programme
NDAP	National Data Analysis Plan
NDMC	National Data Management Committee
PALS	PLHIV-ART Linkages System
PLHIV	People Living with HIV/AIDS
RU	Reporting Unit
SACS	State AIDS Control Societies
SDMC	State Data Management Committee
SI	Strategic Information
SIMS	Strategic Information Management System
SOCH	Strengthening Overall Care for HIV-Patients

## Executive Summary

Under NACP, large volumes of data are being generated as per requirement of the programme and epidemiological tracking needs. NACO encourages the use of this data for evidence based programme planning, research etc at various level. Involvement of a large number of organizations in fighting against HIV/AIDS across the country and the interest and support of a large number of donors and stakeholders emphasizes the need for availability of data to all those who are involved in the program. In addition to this, NACO encourages a culture of research and supports data requests for student dissertation/thesis from across the country.

In order to streamline the process of data management, sharing and use, NACO has periodically developed standardized protocols to be used for data access and sharing at all levels of NACP including facilities that have HIV/AIDS-related information, NACO developed the '**Data Sharing Guidelines**' in 2012. In addition of this, to fully implement the recommendation of the Human Immunodeficiency Virus (HIV) and Acquired Immune Deficiency Syndrome (AIDS) (Prevention and Control) Act, 2017, and to ensure protection of records of HIV-related information of protected persons and prevent it from disclosure, both in the public and private sector, NACO issued the **Data Protection Guidelines** in 2019 to lay guidelines for the adoption of data protection measures from disclosure, procedures for accessing information, provision for security systems to protect the information stored in any form and mechanisms to ensure accountability and liability of persons in the establishment.

Based on the requirement of the programme, these guidelines have been revised from time to time and now, through this document, these two guidelines are being merged and revised to form the **NACP Data Management Guidelines, 2020**.

Based on the sensitivity of NACP data and the need of various stakeholders to access it for routine program management, resource allocation and taking corrective decisions, this guideline provides common, standardized protocols and **Standard Operating Procedures (SOP)** for NACP data management at NACO and SACS for internal sharing as well as a **matrix for approval** by type of data requested for external sharing for students (seeking data for his/her graduate/post graduate dissertation/ PhD thesis work) and other stakeholders. It proposes the constitution of Data Management Committees at various levels to review and approve data-sharing requests, provides an overview of the NACP Data Hub at NACO, protocols to be followed for primary data collection from NACP facilities or beneficiaries etc, data storage, access, sharing, protection, and adverse

event management, if any. The guidelines also lay down provisions for routine monitoring of these activities, which will minimize unauthorized access to sensitive NACP data, and uphold the protection of sensitive data – right from inventory information to patient disease details.

DRAFT

## **1. Introduction**

### **1.1 Background**

The National AIDS Control Organization (NACO) is a Division under the Department of Health & Family Welfare of the Ministry of Health and Family Welfare, Government of India. Through its flagship National AIDS Control Programme (NACP), NACO provides leadership to Human Immunodeficiency Virus (HIV)/Acquired Immunodeficiency Syndrome (AIDS) prevention and control in India through 36 State AIDS Control Societies (SACS) and one Mumbai District AIDS Control Society in States/UTs.

Under NACP, large volumes of data are being generated as per requirement of the programme through various mechanisms including routine programme monitoring, epidemic monitoring exercises such as sentinel surveillance systems, behavioral surveillance surveys, and other evaluations /operations research studies, on a regular basis. The data collected through these mechanisms is used to track progress of HIV/AIDS epidemic in the country and performance of the National AIDS Control Program and for various purposes including effective program management, resource allocation and taking timely corrective decisions.

Due to existence of web-enabled platforms, data transfer has shifted from sequential transfer to direct web transfers, so that information is available at all levels simultaneously, to those who are involved in implementation of National AIDS Control Programme across the country. Adequate measures for data security are therefore needed for restricting access at various levels of stakeholders, and conditional permission protocols need to be established.

### **1.2 Scope and Evolution of data sharing and protection guidelines of NACO**

As an organization which promotes evidence-based decision-making, NACO has continually developed policies, procedures, and training, to ensure that public health data are collected, stored, and used appropriately. Accordingly, policies related to the security and sharing of data are also reviewed regularly and changed as needed. The data standards and the guiding principles for these standards serve as the foundation for a strong, ethical, and dynamic foundation for data management, protection and use.

To address data requests, NACO had formulated the Data Sharing Guidelines in 2012, which was updated in 2015 and subsequently in 2018. In keeping in view of HIV/AIDS (P&C) Act, 2017 NACO had developed Data Protection Guidelines, 2019. These guidelines have been revised from



time to time as mentioned above and now are being revised and merged both the guidelines to form the NACP Data Management Guidelines, 2020. The previous guidelines will cease to exist and for future references, this guideline will be considered final. This guideline is applicable to all establishments generating, collecting, managing and utilizing records of HIV-related information of protected persons.

### 1.3 Types of NACP Data

Essentially all HIV-related information<sup>1</sup> is covered under these guidelines. The following are some examples of the category of these data:

**Published data:** This includes published reports, documents etc. under NACP which are available on [www.naco.gov.in](http://www.naco.gov.in). Most State AIDS control societies have their own websites, and frequently upload program and surveillance reports.

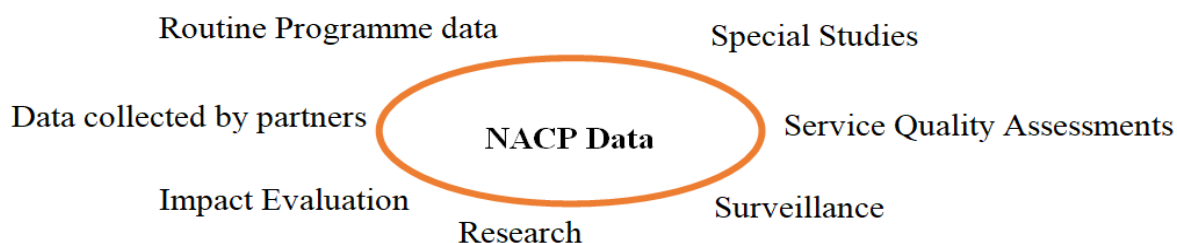
**Aggregate data:** This refers to numerical or non-numerical information that is collected under NACP and compiled into data summaries or summary reports.

**Individual level data without personal identifiers:** This refers to information about individual without relating or linking it to an individual.

**Individual level data with personal identifiers:** This refers to information about individual which can be related/linked to an individual.

### 1.4 Sources of NACP Data

The NACP data is generated through programme data, surveillance, research, special studies/survey, data collected by partners involved in NACP etc.



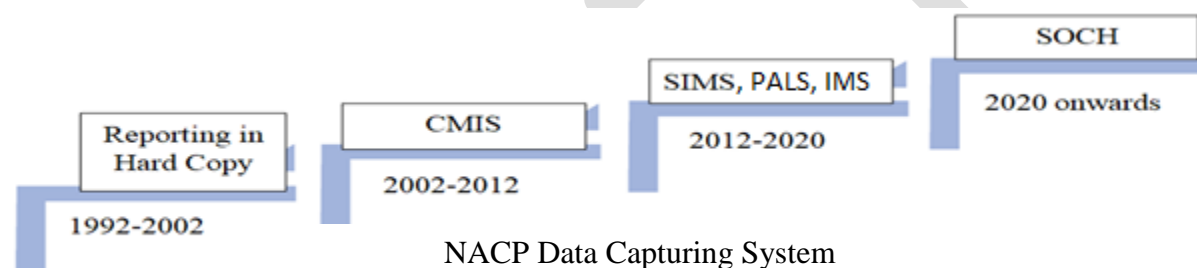
---

<sup>1</sup> “HIV-related information” means any information relating to the HIV status of a person and includes— (i) information relating to the undertaking performing the HIV test or result of an HIV test; (ii) information relating to the care, support or treatment of that person; (iii) information which may identify that person; and (iv) any other information concerning that person, which is collected, received, accessed or recorded in connection with an HIV test, HIV treatment or HIV-related research or the HIV status of that person;

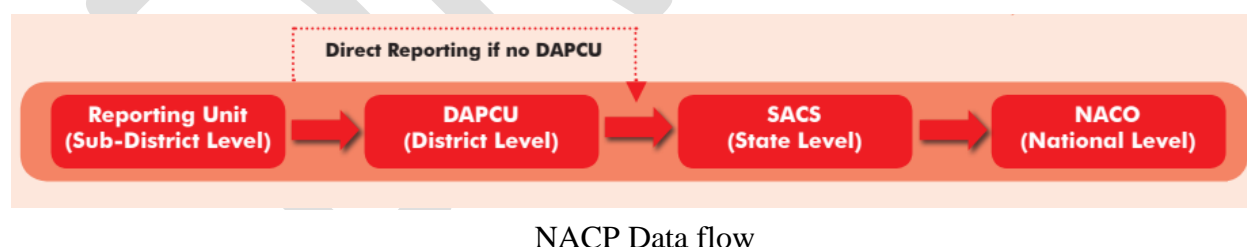


## 1.4 Data Capture Systems under NACP and data flow

The data capture systems under NACP have evolved as per needs of the programme. Under NACP, data is being captured in all aspect of HIV/AIDS which includes prevention, testing, treatment, laboratory services, research, survey, surveillance etc. There are IT-enabled systems for collecting routine programme data from all reporting units across the country. Now, as the country moves towards its 2020 fast track targets and aims to “End of AIDS as a public threat by 2030”, the program data capturing system is being upgraded to a client-centric IT-enabled umbrella platform called SOCH, integrated with all service delivery and embedded supply chain management systems. The illustration below tracks the trajectory of the evolution of NACO’s data systems.



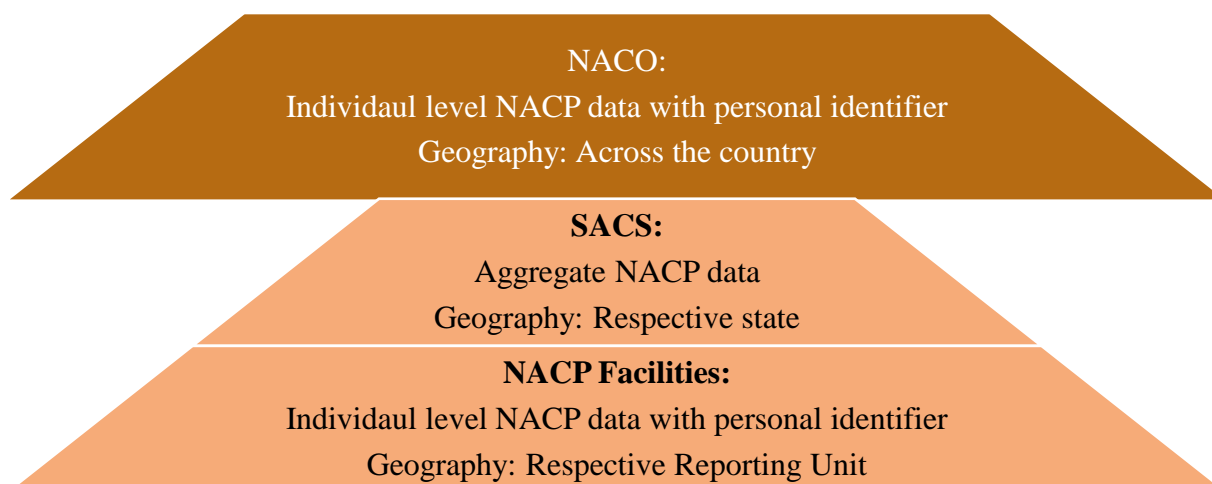
Under the current system, web-based applications within the service delivery system allow for data entry and access at various levels including reporting unit (RU), district and state. Once data is entered at the RU level, all higher levels can view the data in real time. Flow of data is from reporting unit to NACO as given in figure below:



Data transfer has gradually shifted from sequential [Reporting Unit (RU) → District → State → National] transfer to direct web transfer so that information is available to all simultaneously.

## 1.5 Data availability:

The nature and volume of availability of data is different at different level as per hierarchy of the programme and purposes. The details are shown in below figure:



For all data collected through National AIDS Control Program (NACP), NACO/SACS is the custodian. Data in all forms, standard tables, reports as well as raw data will be under the custody of NACO/SACS.

All agencies supporting NACO/SACS in data generation through various processes including routine monitoring, surveillance, research or surveys should handover complete data sets to concerned programme division of NACO after completion of the process/reports. The NACO programme division will share the data to NACP Data Hub at SI Division.

## 2. Key Definition

**Data Management Committee:** The Data Management Committee is a member committee which will review and provide appropriate recommendation to the competent authority on matter related to data management at NACO, SACS and Reporting Unit level.

**Data Hub:** It is a repository of all collected, compiled and approved data under the NACP including data generated through various research studies conducted under the program, surveillance system, survey (conducted by NACO, SACS, or development partners).

**Partners involved in NACP:** Developmental partners/ implementation agency (National & International: government or private organisation /individual), external consultant, IT help desk, interns etc. working for NACO/ SACS have access to NACP data (in any form).

**Facility:** Establishment are those handling HIV related information in government and private setup, i.e. a hospital, maternity home, nursing home, dispensary, clinic, sanatorium or an institution by whatever name called offers services, facilities

	requiring diagnosis, treatment or care for HIV.
<b>Personal identifier:</b> means information about or relating to a natural person who is directly or indirectly identifiable i.e. having name, mobile number, address etc.	
	<b>Data:</b> "data" includes a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by humans or by automated means.

### 3. NACP Data Storage and Protection

In keeping with the **HIV and AIDS (Prevention and Control) Act, 2017**, NACO has laid stringent guidelines and high quality standards for upholding the intent and provisions of the Act related to the confidentiality of HIV-related data. NACO acknowledges the need to use these data with utmost caution and maturity and has provided the following guidelines for data storage and protection.

#### 3.1 Data Storage, Protection and Access

NACP data will be stored in electronic and physical form, based on the requirement of the NACP facilities. For storage in any form, data protection measures shall include procedures for protecting information from disclosure, procedures for accessing information, provision for security systems to protect the information and mechanisms to ensure accountability and liability of persons in the establishment.

- I. Access to all data, including records room or almirahs, registers and reports, data centres or server rooms or computer or any other hardware hosting software/ database on which HIV-related information of protected persons with personal identifier (name, mobile number, Aadhar number etc) is stored should be restricted only to authorized staff members.
- II. Vendors, contractors, consultants and external service providers engaged by establishments should be subject to strict procedures and must have explicit approval and defined period with regard to access to HIV-related information of protected persons by way of formal contract in line with the provisions of 'THE HUMAN IMMUNODEFICIENCY VIRUS AND ACQUIRED IMMUNE DEFICIENCY SYNDROME (PREVENTION AND CONTROL) ACT 2017'. It shall include provision

of undertaking. The terms of the engagement and undertakings given should be subjected to periodic review and audit to ensure compliance. Until and unless required to provide care, support or treatment to the protected person, such access should be restricted to the data without personal identifier.

- III. No unauthorized staff member or vendor or contractors or external service providers should be allowed to watch the working of authorized officer of the establishment while he/she is dealing with HIV-related information having individual identifier of protected persons.
- IV. Filing procedures (both paper and electronic) pertaining to HIV-related information of protected persons should be drawn up and followed.
- V. No papers having HIV-related information of protected persons with their personal identifiers shall be left lying in the authorized staff room or at any other place where unauthorized persons might obtain access to them. Such papers shall be carefully locked in fully secured almirahs or cabinets when not in use.
- VI. Any software or applications for maintaining the HIV-related information of protected persons in the establishment shall be explicitly approved by competent authority of the respective institution.
- VII. To the extent possible, HIV-related information of protected persons held electronically should be stored centrally (e.g. in a NIC data centre, cloud MeghRaj or in establishment's secure server room with documented security in place) with automated backup facility. Data with individual identifier which are readily available via remote access should not be copied to local PCs or to portable storage devices, such as laptops, memory sticks, etc. that may be stolen or lost. When accessing this data remotely, it must be done with relevant access controls in place.
- VIII. In case of data centres or server rooms or Cloud MeghRaj etc., wherever possible, swipe card and/or PIN technology to access the servers in question shall be followed. Such a system should record when, where and by whom the server was accessed. These access records and procedures should be reviewed by competent authority regularly.

- IX. All computer systems, including portable devices (laptops, mobile phones, tablets etc) having HIV-related information of protected persons should be password-protected to prevent unauthorised use of the device as well as unauthorised access to information held on the device. In the case of mobile phones, both a PIN and login password should be used. Manufacturer or operator-provided PIN codes must be changed from the default setting by the user on receipt of the device.
- X. Passwords for hardware, software, databases, etc. should be of sufficient strength to prevent password cracking or guessing attacks. Establishments must also ensure that passwords are changed on a regular basis. A Strong Password must have
- i. Be at least 8 characters in length
  - ii. Contain both upper and lowercase alphabetic characters (e.g. A-Z, a-z)
  - iii. Have at least one numerical character (e.g. 0-9)
  - iv. Have at least one special character (e.g. ~!@#\$%^&\*()\_-=)
- XI. All authorised staff dealing with HIV-related information of protected persons should ensure that PCs or mobiles or tablets or any other hardware are logged off or 'locked' when left unattended for any period of time (e.g. in Windows, using Win + L keys).
- XII. Establishments should ensure that computer systems having HIV related are protected by use of appropriate and up-to-date anti-virus and firewall technologies and it is kept up-to-date to meet emerging threats.
- XIII. Establishments may consider implementation of technologies that will allow the remote deletion of personal data from portable devices (such as mobile phones and laptops etc) should such devices be lost or stolen. A procedure for early notification of such loss should be put in place. This would allow for the disconnection of the missing device from an establishment's email, calendar and file systems.
- XIV. New staff should be carefully oriented and trained on NACP Data Management Guidelines of HIV- related information of protected persons before being allowed to access HIV-related information of protected persons. They must have explicit approval and defined period with regard to access to HIV-related information of protected persons

and shall provide undertaking for protection of data of ‘protected persons’ as per the provisions of the guidelines.

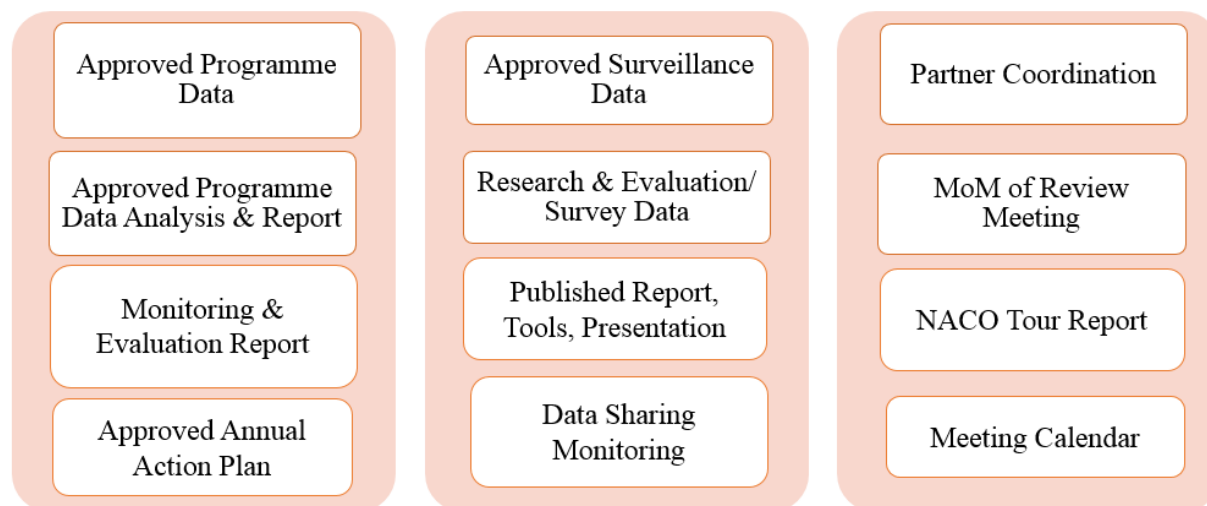
- XV. Staff who retires, get transferred or resign should be immediately de-authorized and barred from access to HIV-related information of protected persons. This shall include barring the access to record rooms or almirahs or data cabinets, data centres or server rooms or Cloud MeghRaj or computers etc as well as removal from the group mailing lists. Relevant changes should also occur when staff are transferred to other assignments internally. It is the responsibility of administration of establishment to ensure that procedures are in place to support this so that notification is provided to the relevant individual(s) or units in a timely fashion.
- XVI. All record rooms or Server rooms should be equipped with fire and security alarms; these shall be tested regularly. There must be a computer back-up or disaster recovery plan. Policies should include plans for a secondary, secure, off-site computer operation that can go into effect in the event of a catastrophic failure at the primary location.
- XVII. There should be an ongoing review of evolving technologies to store data and staff must be trained on updated data storage platforms and data security procedures.

### **3.2 NACP Data Hub**

The NACP Data hub of NACO will be the central repository and collection of component-wise approved NACP data as well as research, surveillance, survey/study etc. data conducted by NACO, SACS, and partners.

### 3.2.1 Overview of NACP Data Hub

The NACP Data hub will contain the following information:



- I. Access: Login id and password to access the data hub will be with all HoD at NACO as per details given in data sharing and transfer section.
- II. Process of data uploading and editing: Data will be uploaded by concerned division of NACO in consultation with SI Division.
- III. Sharing of information available in Data Hub will be done as per details given in data sharing and transfer section.

### 3.3 Data Management Committee and Structure

The Data Management Committee will review and provide appropriate recommendation to the competent authority on data sharing at NACO and SACS level and the committee will also provide appropriate recommendation on the NACP data related matter. These data management committee will supersede all existing committees at NACO, SACS and facility level. The composition of the committee at different levels is as follows:

#### 3.3.1 Composition of the National Data Management Committee at NACO

The National Data Management Committee will be chaired by the senior most head of division (HoD) i.e. Additional Director General/ Deputy Director General and members will be all head of divisions and one subject expert as per need and approval of the chair.

#### 3.3.2 Composition of the State Data Management Committee at SACS

The State Data Management committee will be chaired by the Additional Project Director/senior most officer from programme division and members will be from senior most officers from all divisions of SACS and one subject expert as per need and approval of the chair.



### 3.3.3 All other establishment including NACP facilities (reporting unit) level

Data Management Committee at facility level will be constituted in each establishment which has HIV related information of protected persons. The committee will have 3 members and will be chaired by a senior and relevant officer of the establishment. One of the members shall be representatives from protected persons (e.g. those from the district level HIV positive networks). The committee shall be responsible, accountable and liable for protection of HIV-related information and its sharing of protected persons in their establishment.

### 3.4 Security level of NACP Data

Based on level of security for data sharing, NACP data has been categorized as follows:

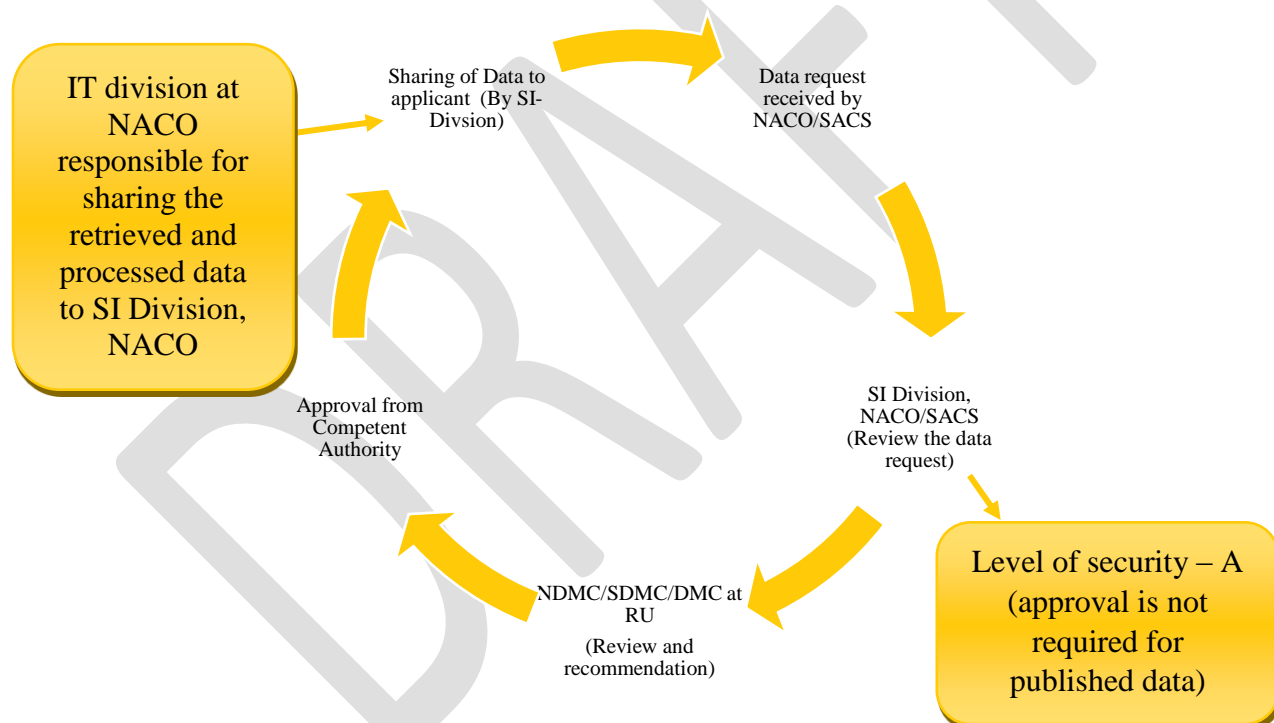
Sl.	Category	Type of NACP Data	Availability
1	A	Published data	NACO/SACS Website/ Concerned programme division of NACO/ SACS
2	B	Aggregate data	NACP Data Hub, Concerned programme division of NACO/ SACS, RU, TSU
3	C	I. Information on procurement & utilization of kits, drugs and other consumables etc. Financial information – total budget sanctioned under various schemes, utilization rates, etc.	NACP Data Hub, Concerned programme division of NACO/ SACS
		II. HSS, BSS, IBBS and other studies/ surveys under NACP.	NACP Data Hub, Concerned programme division of NACO/ SACS
		III. Individual level data without personal identifiers,	IT Division, NACO
		IV. Data/information sharing for order of a court /for legal proceedings	NACP Data Hub, IT Division, NACO & concerned programme division of NACO/ SACS and RU
4	D	I. Individual level data with personal identifiers.	NACO/RU
		II. Direct access to NACP data for Information Technology (IT) related work.	NACO

## 4. NACP Data Sharing and Transfer

NACP data may need to be used by government, semi- government organization, partners, stakeholders, civil society, individuals, research organizations, students etc.

### 4.1 Data sharing and transfer cycle

As explained in the following pictures, data when requested, will be reviewed by the NACO/SACS SI division and forwarded to the concerned Data Management Committee. A positive recommendation by the Data Management Committee will lead the request for approval by the competent authority, and finally, data will be shared by the SI Division (Data Analysis & Use) of NACO in coordination with IT Division/ SI Division of SACS to the requesting individual/organization. The complete cycle of data sharing will be completed by maximum of 45 working days, details is given in table below.



*(Please refer annexure II and III for more details)*

### Timeline for the data sharing

Category	Type of NACP Data	Time
B	Aggregate data	Within 25 working days

C	I. Information on procurement & utilization of kits, drugs and other consumables etc. Financial information – total budget sanctioned under various schemes, utilization rates, etc.	Within 30 working days
	II. HSS, BSS, IBBS and other studies/ surveys under NACP	Within 45 working days
	III. Individual level data without personal identifiers,	Within 45 working days

## 4.2 Matrix of data approval and sharing

**4.2.1** Papers or electronic records containing the HIV-related information of protected persons may be shared with other establishments or persons, without the informed consent of protected person, in following scenarios:

- I. By a healthcare provider to another healthcare provider who is involved in the linkage, care, treatment, support or counselling of such person, when such disclosure is necessary to provide care, support or treatment to that person;
- II. By an order of a court that the disclosure of such information is necessary in the interest of justice for the determination of issues and in the matter before it;
- III. In suits or legal proceedings between persons, where the disclosure of such information is necessary in filing suits or legal proceedings or for instructing their counsel;
- IV. To the officials of the Central Government or the State Government, as the case may be, for the purposes of monitoring, evaluation, surveillance, epidemiological investigations or supervision ;
- V. If it relates to statistical or other information of a person that could not reasonably be expected to lead to the identification of that person; and
- VI. Information Technology (IT) – New application development, existing application data base and source codes maintenance, sharing of IT resources, etc at NACO.

In all other scenarios, no paper or electronic records containing the HIV-related information of protected persons shall be shared or transferred to other establishments or persons without written informed consent of concerned person or his or her representative.

## 4.2.2 Level of security and approving authority for data sharing

- I. Standard email containing the HIV-related information of protected person shall be avoided. Whenever it is required, the file containing the HIV information of protected person shall be encrypted. Staff should ensure that such mail is sent only to the intended recipient. ‘Strong’ passwords must be used to protect any encrypted data. Such passwords

must not be sent with the data it is intended to protect and shall be shared with the intended audience in a separate email. Care should be taken to ensure that the password is sent securely to the intended recipient and that it is not disclosed to any other person.

- II. Papers records containing the HIV-related information of protected persons shall not pass in the ordinary course through the office but shall be seen and dealt with only by persons explicitly authorised in that behalf. Within the establishment, it shall be passed by hand only from one authorised person to another and in sealed covers with clear marking of “Confidential” on envelope. All such sealed covers shall be addressed to an officer by name only. Procedures must be in place for ensuring that the data is delivered only to the person to whom it is addressed, or another officer clearly acting on their behalf, and not any other staff member. Consideration should also be given to the security of files when in transit internally.
- III. When Papers or electronic records sent by post, HIV-related information of protected persons will be closed in double covers of which the inner one shall be pasted or sealed and marked 'confidential' and super-scribed with only the name of the officer by whom it is to be opened. The outer cover will bear the usual official address. Letters or packets containing confidential sent by post shall invariably be registered.
- IV. Data sharing for the research, planning new programme, evaluation, thesis etc for the various components of National AIDS Control Programme shall be taken only by competent authority of National AIDS Control Organization or State AIDS Control Society, due undertaking and approvals in writing shall be in place before sharing the data.

#### **4.2.2.1 Level of security and approving authority for data sharing**

- I. Standard Operating Procedure (SOP) for internal sharing under NACP is given at **annexure I**
- II. For external sharing:
  - A. For students (seeking data for his/her graduate/post graduate dissertation/ PhD thesis work)
  - B. Other than student
    - i. Data request for one state
    - ii. Data request for more than one state

Matrix for approval by type of data requested for external sharing for students is given in table 2 and other applicant is given in table 3 for one state and 4 for more than one state.

**It is important to note that individual/organization receiving data from NACO/SACS neither can share the data with any third party nor can use the data beyond the approved scope without prior authorization from the NACO/SACS. If such action are brought into**

the notice of NACO and found to be correct, then any approval granted to such an individual/organization under given data sharing will be terminated and they will be subjected to penalties, including of but not limited to debarring them for any further data sharing, as suitable by NACO.

**Table 2: Matrix for approval seeking data for Graduation/ Post Graduation dissertation /PhD thesis work (up to two reporting units in same district)**

Level of Security*	Approving Authority	Process
<b>D-I</b>  [If the data required is limited to up to two reporting units/ centres- (accessing available data/ generating fresh data through interviews of beneficiaries)]	In-charge of the Reporting Unit (RU)/ Centre after review by Data Management Committee at RU.	S/he should have to submit letter from HoD and necessary ethical clearance from his/ her institutional review board, for the dissertation/thesis.  S/he should intimate SACS & NACO about the study before starting data collection with copy of information to in-charge of the Reporting Unit (RU)/ Centre.
Approval of Publication	Project Director, SACS After review by Data Management Committee	Request will be processed by SI Division, SACS
If the data required relates to more than two reporting units or district or higher level (either aggregate data or individual data) that is collected through CMIS/SIMS/PALS/SOCH or any other data collection /reporting mechanism under NACP, the student should approach SACS/NACO with data request. In such case, the protocol as given in table-3 will be followed. <i>*Please refer section 3.4 for details of Level of Security of data</i>		

**Table 3: Matrix for approval by type of data requested for external sharing (other than NACO, SACS and partners) for one state.**

Level of Security*	Approving Authority	Process
A	Approval not required, if available on website, If not available on website, Respective HODs of SACS	Undertaking not required
B	Project Director, SACS After review by State Data Management Committee	Undertaking required. Request will be processed by SI Division, SACS
C-I	Project Director, SACS after review by State Data Management Committee	Undertaking required. Request will be processed by SI Division, SACS

C-IV	Project Director, SACS	Request will be processed by SI Division, SACS
Approval for Publication (if the name of Government Official working at NACO/SACS used as author)	Project Director, SACS After review by State Data Management Committee	Request will be processed by SI Division of SACS
<p>Individual level data (without personal identifier) fall in categories C-II &amp; C-III will be shared by NACO as given in table 4.</p> <p>Individual level data (With personal identifier) of beneficiaries of various components under NACP cannot be shared, thus in this regard no proposal will be accepted (except for order of a court/ in legal proceedings).</p> <p><b><i>*Please refer section 3.4 for details of Level of Security of data</i></b></p>		

**Table 4: Matrix for approval by type of data requested for external sharing (other than NACO, SACS and partners) for more than one state.**

Level of Security*	Approving Authority	Process
A	Approval not required, if available on website, If not available on website, Respective HODs of NACO/ SACS	Undertaking not required
B	Joint Secretary, NACO After review by National Data Management Committee	Undertaking required. Request will be processed by SI Division (Data Analysis & Use) NACO.
C-I	Director General, NACO after review by National Data Management Committee	Undertaking required. Request will be processed by SI Division (Data Analysis & Use), NACO.
C-II & III	Director General, NACO after review by National Data Management Committee	Undertaking required. Request will be processed by SI Division (Data Analysis & Use), NACO
C-IV	Director General, NACO	Request will be processed by SI Division (Data Analysis & Use), NACO.
Approval for Publication (if the name of Government Official working at NACO/SACS used as author)	Director General, NACO After review by National Data Management Committee	Request will be processed by SI Division (Data Analysis & Use), NACO.
<p>Individual level data (With personal identifier) of beneficiaries of various components under NACP cannot be shared , thus in this regard no proposal will be accepted (except for order of a court/ in legal proceedings)</p>		

*\*Please refer section 3.4 for details of Level of Security of data*

#### **4.3 Data sharing process:**

As recommended by Data Management Committee and approved by competent authority, data will be shared by SI Division (Data Analysis & Use) in coordination with IT division of NACO and SI Division of SACS to the requesting individual/organisation.

#### **5. Data disposal at NACO/SACS/RU**

- I. Establishment shall have standard procedures in place in relation to disposal of files containing HIV-related information of protected persons, as per the government norms. Full documentation about all data disposal shall be maintained.
- II. Procedures should also be put in place in relation to the secure disposal of computer equipment (especially storage media) at end-of-life. This could include the use of erasers and physical destruction devices, etc.
- III. If third parties are employed to carry out such disposal, they must contractually agree to the establishment's data protection procedures and ensure that the confidentiality of such data is protected.

#### **6. Risk Mitigation/ Adverse events management**

- I. Adverse events in the form of breach in data protection mechanism may happen in few scenarios including but not limited to human error, hacking attack etc. Each establishment shall have adverse event management plan to respond to such unwanted incidence. The adverse events management plan shall cover aspects of identification and reporting, review and actions for containment, recovery and notification.
- II. Staff member or vendor or contractors or external service providers shall report any case of breach in data protection to the "Data Management Committee" within 72 hours of incidence coming to his or her notice. He or she shall provide the details of the incident to the extent possible, like including the probable date and time the incident occurred, the date and time it was noted, how it was noted, description of the incident, details of any database software or applications systems involved, log files, etc.
- III. Concerned Data Management Committee shall immediately review the risk associated with data breach in terms of what type of data is involved, does it has individual identifier, how many individuals data is affected, are there any protections in place (e.g, encryption) etc. Immediate actions for the containment of data breach shall be taken based on the review.
- IV. Concerned Data Management Committee will also inform about such incidents with



action taken report to the concerned designated authority<sup>2</sup>”.

## **7. Data security monitoring at NACO, SACS and RUs**

Responsibility for data security will be with each and every establishment having data of protected people. In case of NACP facilities, responsibility of data security will be also with concerned programme division at NACO and SACS.

Access to files/data containing HIV-related information of protected persons will be monitored by SI Division (Data Analysis & Use) and IT Division at NACO and DD (SI) or equivalent at SACS on regular basis. DD (SI)/equivalent officer of respective SACS have to prepare monthly report on data security and have to submit the report to SI division (Data Analysis & Use) of NACO by 10<sup>th</sup> of every month.

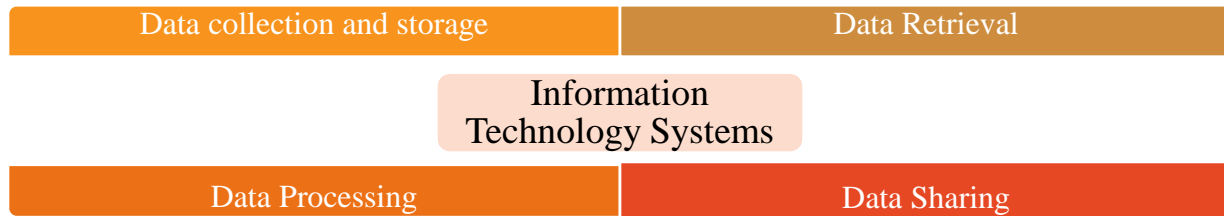
Key points:

- I. Every establishment which has HIV-related information will monitor the implementation of NACP Data Management Guidelines within the establishment. It will include monitoring of “unauthorised sharing or access to, or alteration, disclosure or destruction of the containing HIV-related information of protected persons as well as their accidental loss or destruction”. Technological solutions shall be considered for supervising all external visitors whenever they are in record rooms or Server rooms.
- II. For monitoring the access (whether internal or external) to databases with HIV-related information of protected persons, system technology shall have functionalities to monitor trail for data edits (addition, deletion etc), ‘view’ or ‘read’ access. In systems where such functionalities does not exist, it should be investigated, as a matter of urgency whether such functionality can be enabled in existing systems. If such functionality cannot be enabled and the risk of inappropriate access is sufficiently high, such systems should be scheduled for removal from use and replaced by systems with appropriate functionality for monitoring.
- III. Access to files containing HIV-related information of protected persons should be monitored by supervisors on an ongoing basis. Staff should be made aware that this is being done.

---

<sup>2</sup> Director General, NACO, Joint Secretary, NACO and Project Director, SACS

## 8. Role of Information Technology



**Data Collection and storage:** Information Technology division is the custodian of Information Technology/Management systems used by the frontline health care workers for the data collection and storage under NACP.

**Data Retrieval:** Up on receipt of data request, stored data to be retrieved by IT division as Information Technology/Management Systems application Admin or database admin using query languages.

**Data Processing:** Processing and manipulation of retrieved data to make it more informational as per the data request.

It is about constructing a data set from one or more data sources to be used for further exploration and processing.

**Data Sharing:** IT division at NACO responsible for sharing the retrieved and processed data to SI Division, NACO.

## Standard Operating Procedure (SOP) for NACP Data Management at NACO and SACS

This SOP will streamline the National AIDS Control Programme data access and sharing at NACO/ State AIDS Control Society (SACS). For partners working with NACO/SACS this SOP will streamline primary data collection from National AIDS Control Programme (NACP) facilities or beneficiaries as well as sharing of NACP data with partners.

### 1. Definitions:

#### Approving authority:

At NACO: Director General and Joint Secretary

At SACS: Project Director

**Head of Division (HoD):** Senior most officer and in-charge of respective programme division at NACO. Senior most officer and charge of respective programme division at SACS.

**SACS:** It includes all SACS and Mumbai Districts AIDS Control Society.

**Officers:** Permanent and contractual staffs in all divisions of NACO who have access to National AIDS Control Programme (NACP) data.

Permanent and contractual staffs in all divisions of SACS who have access to NACP data.

**Data sharing organization:** Data sharing will be done only by NACO and SACS as per NACP Data management Guidelines, 2020.

In case of student dissertation/thesis, respective reporting unit may share the data as per the guidelines.

**National Technical Support Unit (NTSU)/Technical Support Unit (TSU):** It includes NTSU at national and all TSUs at state involved in technical assistance to the NACO/respective SACS in implementation of National AIDS Control Program. NTSU/TSU cannot share data to any organization including NTSU/TSU management agency.

#### Partners:

Government Institutions involved in NDAP/Research/Surveillance and other activities as per MoU with NACO.

UN Agencies/Bilateral/Donor/Implementing Partners.

This will not include Technical Support Units engaged by NACO for their given mandate.

**NACP Data hub:** NACP Data hub of NACO has collection of approved NACP data as well as research, surveillance, survey/study data conducted by NACO and SACS. The hub will be managed by SI Division under the leadership of DDG (SI). For details refer section 3.2 of the guideline.

### 2. Scope

This SOP applies to all personnel involved in NACP data handling at NACO, SACS, and partners.

In addition of this it will also streamline the primary data collection from NACP facilities and beneficiaries by the partners.

### **3. Goal**

Keeping in view the HIV and AIDS (Prevention and Control) Act, 2017, there is a need to use NACP data with utmost caution and maturity. The main goal of this SoP is to streamline the data sharing at NACO & SACS (interdivision and with partners) and to restrict unauthorized data access, sharing, retrieval etc.

### **4. Collection of data from beneficiary under NACP:**

**4.1** It is mandatory to maintain privacy and take consent before collecting data from beneficiary under the NACP. Following provisions must be indicated while seeking consent

- Beneficiary may withdraw her/his consent at any point of time during the process, which means, her/his data will not be collected/entered in data base.
- Beneficiary may access/update/correct the information which is collected under the programme by visiting concerned NACP facility.
- There should be clear information as to with whom (individual/organisation) collected data will be shared.
- In case the information is required to be shared beyond the individual/organisation mentioned in consent, there is need to take additional consent before sharing the information.

**4.2** In due course of time if the beneficiary wishes that her/his data should be forgotten/disabled from the data base, this right shall be entitled to them.

**4.3** All NACP facilities handling HIV related data should have a proper mechanism in place to facilitate implementation of all aforementioned provisions and also to ensure capacity building of officers/staffs on 'Data Management' with special focus on aspect of 'withdrawal of consent' and 'right to be forgotten'.

This mechanism to be routinely monitored by respective Data Management Committee at facility level.

Records containing the HIV-related information of protected persons may be shared with other establishments or persons, without the informed consent of protected person as given in section 4.2.1 of the guideline.

## 5. Collection of primary data from NACP facility or beneficiary by partners:

Type of Information	Level of security	Approving Authority	Process
Collection of primary data from NACP facility or beneficiary by partners (information other than available in records at NACP facilities)	D-I	Director General, NACO	Request will be processed by concerned programme division of NACO as per standard procedure with copy for information to SI Division (Data Analysis & Use).  Data collected as part of data collection under standard MoU (e.g. research, surveillance etc.) will be shared by institute/ organisation/ agency in accordance with terms specified in the MoU. Once data collection/activity is over, raw dataset along with final dataset will be submitted to programme division concerned. The NACO programme division will share the data to NACP Data Hub at SI Division.

## 6. NACP data access at NACO and SACS

Head of Division at NACO & SACS will have access to NACP data available in CMIS/SIMS/PALS/IMS/SOCH or other related software and DDG (SI & IT) will be the overall in charge including NACP Data hub.

## 7. Process of review and approval for NACP data sharing:

Process of review and approval for data sharing is given in table below:

Level of Security <sup>\$</sup>	Approving Authority	Process
<b>1. Inter-division data sharing (for officers working in NACO, SACS and TSU)</b>		
A	Approval not required, if available on website, If not available on website, Respective HODs of NACO/ SACS	E-mail/ letter required
B & C-I	Respective HoD of NACO/ SACS	E-mail/ letter required
C-II & III	Joint Secretary, NACO  After review by National Data Management Committee	E-mail/ letter required from respective division of NACO and SACS.  Request will be processed by SI division (Data Analysis & Use), NACO
<b>2. NACP data sharing to partners working with NACO and SACS</b>		
A	Approval not required, if available on website,	E-mail/ letter required

Level of Security <sup>\$</sup>	Approving Authority	Process
	If not available on website, Respective HODs of NACO/ SACS	
B & C-I	Joint Secretary, NACO  Project Director, SACS	MoU with NACO/ Approval from competent authority* and undertaking required.  Request will be processed by SI division (Data Analysis & Use) of NACO/ SI Division of SACS. Responsibility of data security will be concerned programme division of NACO and SACS
C-II & III	Director General, NACO  After review by National Data Management Committee	MoU with NACO/ Approval from competent authority* and undertaking required.  Request will be processed by SI division (Data Analysis & Use) of NACO  Responsibility of data security will be with SI division (Data Analysis & Use) of NACO
Approval for Publication (if the name of Government Official working at NACO/SACS used as author)	Director General, NACO  Project Director, SACS  After review by concerned Data Management Committee	MoU with NACO/ Approval from competent authority*.  Request will be processed by SI division (Data Analysis & Use) of NACO/ SI Division SACS
<p>*Partners working with NACO/SACS must have approval letter containing name of person, designation, period and purpose for access to HIV-related information from the competent authority of NACO &amp; SACS.</p> <p>Each SACS have to submit details of data shared with partners on monthly basis to SI Division (Data Analysis &amp; Use), NACO.</p> <p>Individual level data with personal identifier of beneficiaries of National AIDS Control Programme cannot be shared with partners, thus in this regard no proposal will be accepted.</p>		
<b>3. Direct access to NACP data for Information Technology (IT) related work</b>		
Must have MoU with NACO/approval of access to HIV-related information of protected persons/beneficiaries under the NACP from the competent authority stating name of person, designation, and period. They must have to maintain logbook of data accessed, downloaded clearly stating reasons, date and time with signature.		
D-II	Joint Secretary, NACO	I. MoU/Undertaking from project lead and the team working on the

Level of Security <sup>\$</sup>	Approving Authority	Process
		<p>project of the partner organisation is required.</p> <p>II. Undertaking by Original Equipment Manufacturer (OEM) giving the details of the data being fetched from the machine and the details of the server where data is uploaded along with the server location.</p> <p>III. Undertaking by Original Equipment Manufacturer (OEM) mentioning none of the individual's testing Data (bar code and test result details) is being fetched from the machine.</p> <p>Responsibility of data security will be with coordinating officer of NACO (not below Deputy Director Level)</p>
<i><sup>\$</sup>Please refer section 6.3 for details of Level of Security of data</i>		

## 8. Data sharing and monitoring:

### 8.1 Data Sharing

As recommended by concerned Data Management Committee and approved by competent authority, data will be shared by SI Division (Data Analysis & Use) of NACO and SI Division of SACS to the requesting individual/organisation.

### 8.2 Monitoring of Data sharing:

Responsibility for data security will be with concerned establishment, IT Division and concerned division of NACO and SACS.

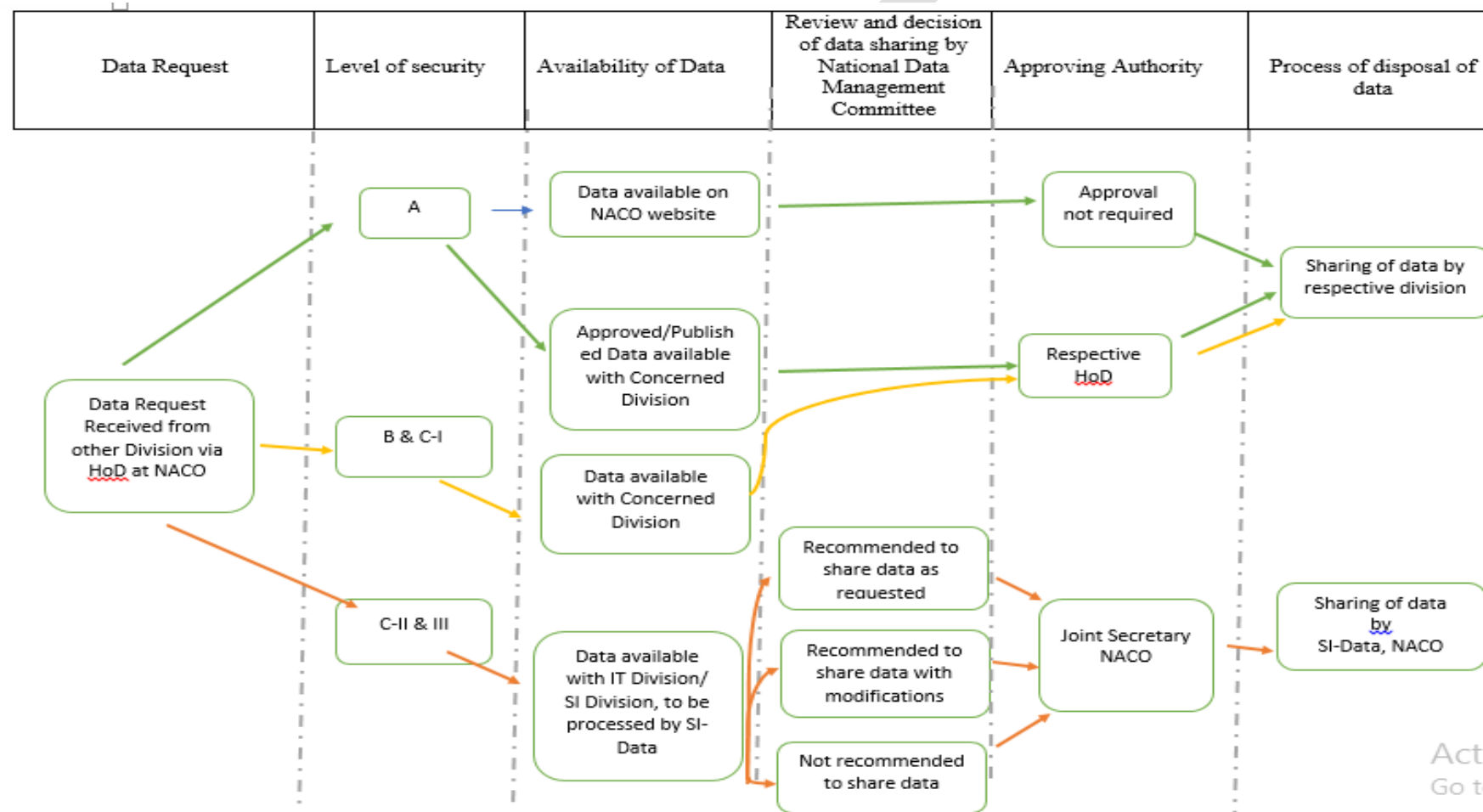
Access to files/data containing HIV-related information of protected persons will be monitored by SI Division (Data Analysis & Use) at NACO and DD (SI) at SACS on regular basis. DD (SI) of respective SACS have to prepare monthly report on data sharing and have to submit the report to SI division (Data Analysis & Use) of NACO by 10<sup>th</sup> of every month.

## 9. Applicable Act, Guidelines and Office Order:

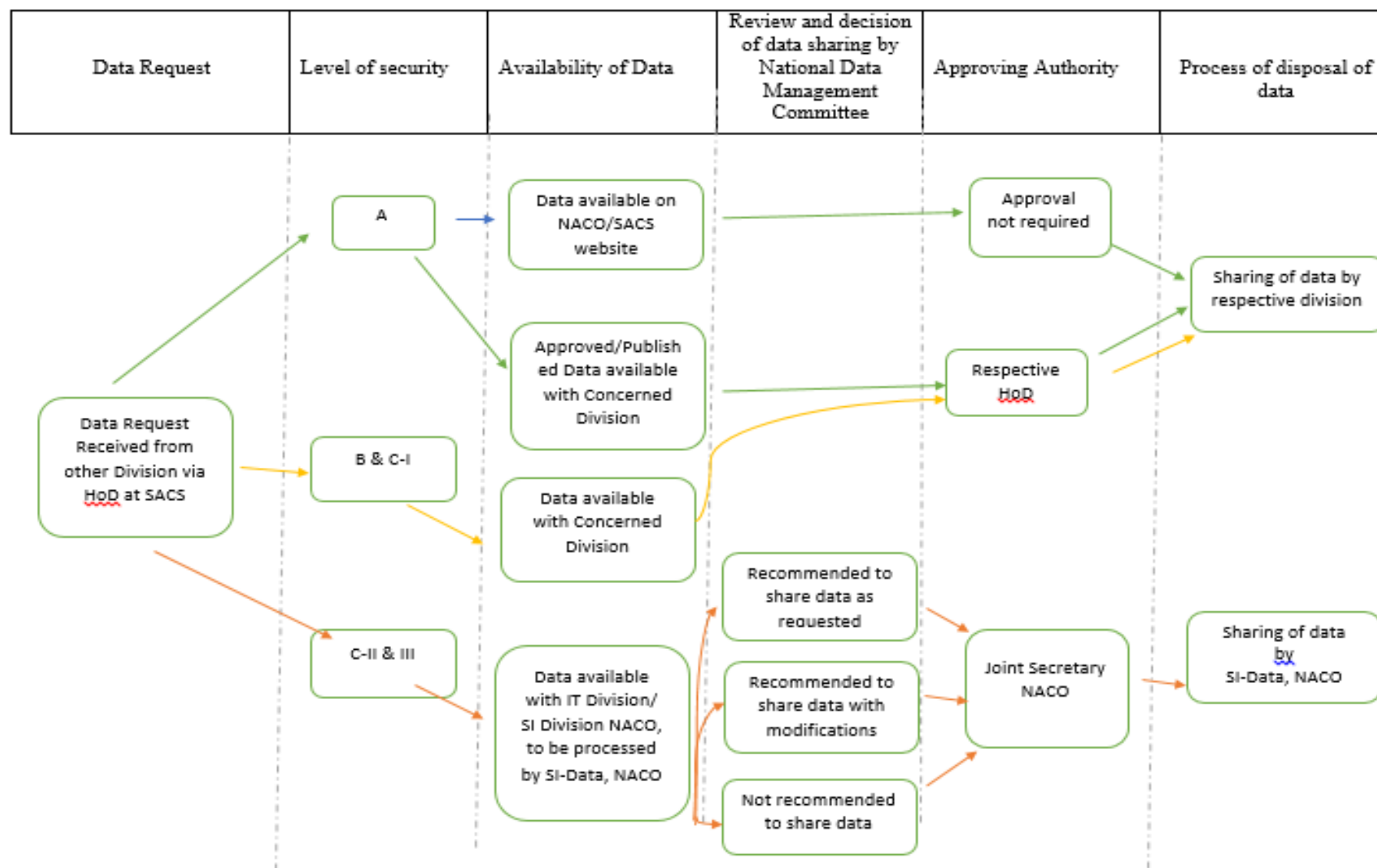
1. HIV and AIDS (Prevention and Control) Act, 2017
2. NACP Data Management Guidelines, 2020



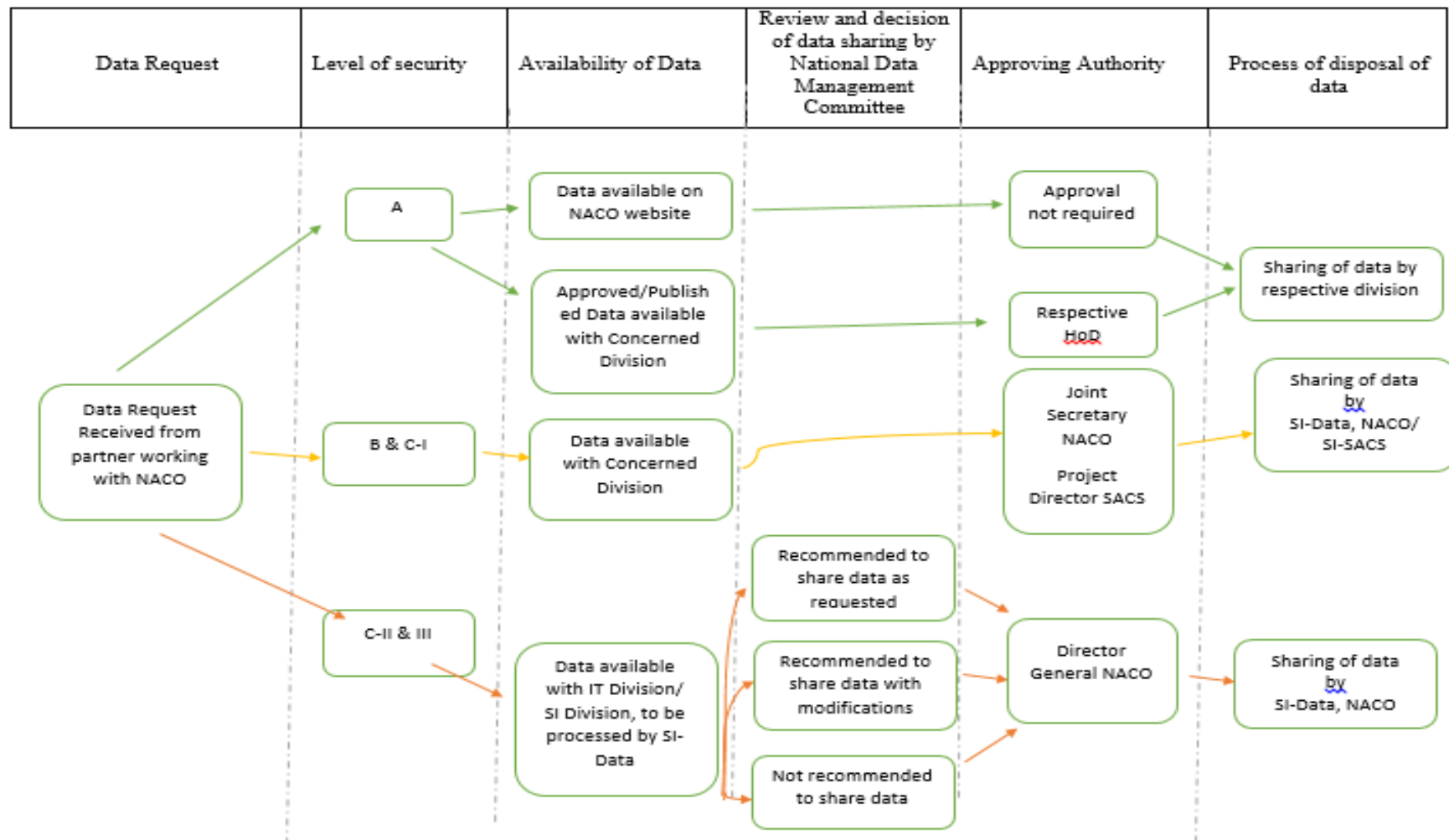
### Process of review and approval for internal NACP data sharing at NACO



## Process of review and approval for internal NACP data sharing at SACS for SACS and TSU officials



### Process of review and approval for NACP data sharing to partners



**Annexure -IV**  
**Format for Data Request**

Name and Address of the Individual/Institute/Agency Requesting – NACP Data/ Access to NACP data for programme/IT related work: -----  
-----

Purpose:

- I. Planning new programme
- II. Program management / evaluation
- III. National Data Analysis Plan
- IV. Research
- V. Surveillance
- VI. Information Technology (IT) – New application development, existing application data base and source codes maintenance, sharing of IT resources, etc at NACO.
- VII. Others (Please specify) -----

Whether protocol of the study/proposal is enclosed: Yes / No

Details of data request (Explain how the requested data would be used):  
-----

Define the data requirement

- I. Component on which information required:
- II. Geographical area:
- III. Time period:
- IV. Level of data –Aggregate/ individual level:
- V. Indicators/ Variables required (complete list with details):
- VI. Any disaggregation required:

Date:

Signature:

Name & Designation:

Institution:

**Format for Undertaking**

I/We----- (Name),  
 working as----- (Designation), in-----  
 -----  
 ----- (Complete Name and Address of Institution/ Organisation), am/are  
 involved in the study/analysis titled “-----  
 -----  
 -----” from-----to----- (time period).

I hereby declare that the data that I am provided access to, under the above- mentioned study/ analysis will be used only for the purpose of the work mentioned hereinabove and only in the manner that National AIDS Control Organisation (NACO) authorizes and permits. I expressly acknowledge and agree that without prejudice to all the available legal remedies, I am also liable to administrative action in case the data is used for any purpose beyond the scope of this study. I will not share the data with any one, or publish the research data without prior written consent/permission from NACO and shall maintain the confidentiality of all Confidential Information. I shall submit a copy of all the data files, analysis papers and reports generated as a part of this analysis work to NACO at the end of the study/analysis. Any publication out of this analysis will have prior NACO review. Any publication, document, and/or paper arising out of this analysis will be jointly owned.

Date:	Signature: Name & Designation: Institution:
Contact Details: Mobile Number:-----Telephone Number:----- Email:-----	
<b>(Signature of the Head of Institution/Organisation)</b> <b>Name of the Head of Institution/Organisation:</b>  <b>Official Seal:</b>  <b>Date:</b> <b>Place:</b>	

## Format for Non-disclosure/confidentiality form

The data/ information/ material to which the partner organisation/individual is provided access to under the MoU, shall be used only for the purpose of the assignment under the MoU. It shall not be used for any purpose beyond the scope of the MoU. The data/ information/ material shall not be shared with any one, nor published without prior permission from NACO/SACS. The outcomes from the project under the MoU, interim or final, in the form of technical analytic outputs, conclusions, scientific articles, papers, presentations, abstracts, or in any other form shall not be published/presented without prior permission from NACO/SACS, even after the termination of the MoU. All the data files, analysis papers, reports and any other technical output generated as a part of this project shall be submitted to the NACO/SACS at the end of the MoU.

I/We----- (Name),  
 working as----- (Designation), in-----  
 -----  
 ----- (Complete Name and Address of Institution/ Organisation), am/are  
 involved in the project “-----” from-----  
 ----- to----- (time period).

I hereby declare that the data that I am provided access to, under the above- mentioned project will be used only for the purpose of the work mentioned hereinabove and only in the manner that National AIDS Control Organisation (NACO) authorizes and permits. I am also liable to administrative action in case the data is used for any purpose beyond the scope of this work. I shall maintain the confidentiality of all information which I have access during the project period and also after the completion of allotted work.

Date:	Signature:_____Name & Designation:_____
	Institution:_____
Contact Details:	
Mobile Number:-----Telephone Number:-----	
Email:-----	
(Signature of the Head of Institution/Organisation with official seal, date and place)	
Name of the Head of Institution/Organisation:	

## **Annexure –VII**

### **Checklist for data request**

1. Completely filled and signed data request form as given at annexure-IV
2. Detailed protocol of the study indicating complete list of indicators,
3. Relationship with NACO (MoU or other, if any)
4. If partner of NACO, details of engagement with NACO
5. Local IRB approval (if applicable).
6. Completely filled and signed undertaking as given at annexure-V
7. Filled and signed non-disclosure/confidentiality form (if applicable) given at annexure-VI
8. Any other supported document, if applicable

DRAFT

**In case of any query please contact**

**Deputy Director General**  
Strategic Information Division  
National AIDS Control Organisation  
Ministry of Health & Family Welfare  
Government of India

\*\*\*\*\*