DATA PROTECTION GUIDELINE OF NATIONAL AIDS CONTROL PROGRAMME

1. Introduction

Every establishment, including those in the private sector,[1] keeping the records of HIV-related information[2] of protected persons[3] shall adopt data protection measures in accordance with the guidelines to ensure that such information is protected from disclosure. Data protection measures shall include procedures for protecting information 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. This guideline is in conformity with the Human Immunodeficiency Virus (HIV) and Acquired Immune Deficiency Syndrome (AIDS) (Prevention and Control) Act, 2017 (16 of 2017). This national guideline is applicable for both public and private sector.

2. Overview

This document provides guidelines on how HIV-related information of a PLHIV will be stored, handled, accessed and protected under the following headings: -

I. Data Protection Committee
II. Data access and storage
III. Data sharing & transfer
IV. Data disposal
V. Data protection monitoring
VI. Adverse events management

2.1 Data Protection Committee

A data protection committee (DPC) shall be constituted in in each establishment which has the HIV-related information of protected persons. The committee shall have3 members and shall be chaired by a senior and relevant officer of the establishment. One of the members shall be representatives from protected persons (eg, those from the district level HIV positive networks).The committee shall be responsible for the accountable and liable for protection of HIV-related information of protected persons in their establishment.

2.2 Data access and storage

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.

---

[1] "Establishment" means a body corporate or co-operative society or any organisation or institution or two or more persons jointly carrying out a systematic activity for a period of twelve months or more at one or more places for consideration or otherwise, for the production, supply or distribution of goods or services;

[2] (l) "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;

[3] "Protected person" means a person who is— (i) HIV-Positive; or (ii) ordinarily living, residing or cohabiting with a person who is HIV-positive person; or (iii) ordinarily lived, resided or cohabited with a person who was HIV-positive;

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'. 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 unauthorised staff member or vendor or contractors or external service providers should be allowed to watch the working of authorised 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 authorised staff room or at any other place where unauthorised 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
    a. Be at least 8 characters in length
    b. Contain both upper and lowercase alphabetic characters (e.g. A-Z, a-z)
    c. Have at least one numerical character (e.g. 0-9)
    d. 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 data protection 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 data protection 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.

2.3 Data Sharing and transfer

I. 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:
   a. 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;
   b. 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;
   c. 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;
   d. 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
   e. 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.

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.

I. 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 State AIDS Control Society or National AIDS Control Organization in accordance with the

July 2015 Data Sharing Guidelines of National AIDS Control Organisation[4]. In all such scenario, as prescribed in the data sharing guidelines, due undertaking and approvals in writing shall be in place before sharing the data.

II. 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 toprotect 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.

III. 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.

IV. When Papers or electronic records sent by post, HIV-related information of protected persons shall 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.

2.4 Data disposal

I. Establishment shall have standard procedures in place in relation to disposal of files containing HIV-related information of protected persons. 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.

2.5 Data protection monitoring

I. Every establishment which has HIV-related information shall monitor the implementation of data protection guidelines within the establishment. It shall include monitoring of "unauthorised 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

[4]http://naco.gov.in/sites/default/files/Data%20Sharing%20Guidelines_%2013%20July%202015.pdf

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.

2.6. 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 Protection 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. Data protection committee (DPC) 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. DPC shall also inform about such incidents with action taken report to the concerned designated authority".