

STANDARD OPERATING PROCEDURES

PEPFAR Health Information Systems User Validation

Version 2.5

December 2021

Version History

Version	Date	Description	Author(s)
1.0	June 15, 2020	Initial creation of document	PEPFAR HIS Team
1.1	July 10, 2020	Modifications based on report, simplified and removed suggested appendixes.	PEPFAR HIS Team
1.2	July 13, 2020	Minor edits	PEPFAR HIS Team
1.3	March 15, 2021	Updates to organization and process	PEPFAR HIS Team
1.4	June 1, 2021	Moved to standard template format Modified text	PEPFAR HIS Team Maria Rein
2	November, 16, 2021	Restructuring of the DLT user validation SOP, in SOP of validation of users of the PEPFAR supported web based HIS supported by the Helpdesk and framing of legal aspects	Marcelino Mugai
2.1	November, 17, 2021	General review and English translation	Banucho Cassamo, Elísio Macia, Vania da Mira Afonso and Zainabe dada
2.3	November, 30, 2021	General review and semi-final editing	António sitoí
2.4	November, 30, 2021	Final review and approval	Alessando Campione
2.5	December 8, 2021	Edits	Maria Rein

1. Introduction

This Standard Operational Procedure (SOP) is for validating users of PEPFAR supported web based health information systems supported by the Helpdesk. This document aims to minimize the risk to unauthorized access to patient and facility health information stored in these systems. This SOP aligns with CDC Mozambique HIS policy and by Mozambique law number 5 of the article 63 of law 03/2017 (Electronic Transaction's law) - "The Data processor must protect personal data against risk, loss, unauthorized access, destruction, use, modification or disclosure".

The user validation process of HIS is performed routinely to ensure approved users have access to the system and all users have signed non-disclosure agreements, indicating the user understands the importance of keeping the health information they have access to is kept confidential and secure.

2. Purpose

Users with access systems might leave an organization and the organization might forget to notify PEPFAR, the former employee no longer needs access to the system and the employees access should be removed. The following standard operating procedure will ensure there is a biannual validation process to ensure only authorized users have access to the system. It will also ensure that active users agreed and signed non-disclosure agreements.

The process must start at the beginning of the COP year (October) and in March.

3. Scope

The process for providing a user access to the System is not within the scope of this document;

The user validation process covered in this SOP does not cover users who exclusively use the paper component of these systems, considering a user as “one who uses electronic system”, pursuant to the definition used in law nº 03/2017, the Law of electronic transactions;

Matters on Access to paper-based systems are governed by the different legal instruments instituted by the Government of Mozambique and adopted at all levels of the Ministry of health, taking as an example the spirit of the Health Information Policy as mentioned in the chapter of legal framework of this SOP.

This SOP doesn't address distributed system currently.

4. Background

To access the System, a user requests access to the system through the system focal point within their organization. The request is submitted to the Helpdesk. Upon completion of system training, the user is required to signing a non-disclosure agreement (NDA). Following the completion of the NDA, users are assigned a username and a password by the HIS implementing partner system administrator.

When an employee with access to a system leaves an organization, it is the responsibility of the organization focal point to notify the PEPFAR team and HIS implementing partner/MoH via the Helpdesk when the employee has departed. Following the notification, the user account should be set to “inactive”. The system will be updated and the date the user was removed will be noted. It will be verified the user no longer can access the System.

Each system contains an auditing log which indicates when a user was added, their user name, email and organizational affiliation of the user, their access type, the status of their account (active/inactive), the date they were set to inactive status.

5. Legal framework

According to the section ii, line "b" of number 5.3 (Rights and Data access) of Health Information Policy, version of January 2021, "people who access any personal health data adhere to specific deontological norms; at least, these norms must: Be explicitly mentioned in the individual description tasks".

According to the section ii and IV of number 6.1 (Proprietary actions and responsibilities) from Health Information Policy, version of January 2021, the Health services (Central Level) has the responsibility to "create a file in each health facility containing confidentiality terms assigned by eligible providers" and "include one consent term resumed and intelligible (for someone with 4 year of basic education) in all forms that record the patient individual data in the health facilities" respectively.

Each HIS have different types of access to the system, but a user access to the system has two settings:

- Active – the user can access the system;
- Inactive – the user no longer has access to the system.

6. Supported Systems, responsibility for creating user accounts, and type of users

It is the responsibility of the HIS implementing partner, responsible for the maintaining the system, to add and remove users from the system. Clinical and community implementing partners, do not have administrative access to add or remove users from systems This is to ensure the SOP is being implemented and user validation is managed to avoid unauthorized access to the systems.

#	System name	Organization Responsible for user Account Creation	Type of users
1	DREAMS Layering Tool	FGH	PEPFAR supported clinical partners, community based organizations (CBOs) and PEPFAR.
2	GBV eIMD	JEMBI	GBV Focal Points at Central, Provincial, District and HF levels of the MOH, Health provider at the HF level and PEPFAR supported IP providing support for GBV
3	GBV Mapping Tool	JHPIEGO	To de determined
4	VMMC System	JEMBI	PEPFAR supported clinical partners providing VMMC services and MISAU VMMC Program
5	VMMC Demand Creation App	FGH	PEPFAR supported clinical partners providing VMMC services and MISAU VMMC program
6	MOZART Database	PEPFAR HIS team	PEPFAR Strategic Information (SI), PEPFAR Surveillance and Epidemiology, PEPFAR HIS, INS and MISAU DNAM / HIV Program, MISAU DPC/DIS

7. Roles and Responsibilities

It is the responsibility of the IP organization focal point to provide updates when a user has left the organization;

It is the responsibility of the IP organization focal point to provide updates of new users working in the organization;

It is the responsibility of the IP organization focal point to ensure users have signed non-disclosure agreements;

It is the responsibility of the Helpdesk to validate the users biannually;

It is the responsibility of the Helpdesk to store the signed NDA for each system;

It is the responsibility of the HIS implementing partner overseeing each of these systems to request removal/ remove users identified as no longer being affiliated with the organization and to ensure unauthorized access to the system does not occur;

It is the responsibility of the Helpdesk to collaborate with the PEPFAR HIS team, implementing partners and MOH to ensure there is a focal point for user validation and to support user validation activities.

8. Procedure for Validating DREAM, e-IMD GBV, VMMC and MOZART I Users

Every six months (i.e., October and March) the Helpdesk in collaboration with PEPFAR HIS, MOH and implementing partners will validate system users.

PEPFAR HIS will provide a list of organizational focal points.

The organization focal point is responsible for validating the list of users within their organization.

Once the organization focal point list has been received, the HIS implementing partner, maintaining the system, will provide the Helpdesk a list of all current users with a status of "ACTIVE".

The Helpdesk will organize the list of each system by organization and send an email to the organizational focal point, with a copy to PEPFAR HIS f requesting they validate the users within 5 business days.

Once the organizational focal point has validated the list, the Helpdesk team will ensure an NDA is on file for each user.

If an NDA is not on file, they will request an NDA be submitted.

If a user has been identified as no longer with the organization, the Helpdesk will compile a list of all users to be set to "inactive" status.

At the end of the process, the HIS Implementing partner will provide a list of all "inactive users" to ensure all users no longer affiliated with the organization, during the review period, were set to inactive status.

The system organizational focal point is responsible for validating all users within their organization. If an organizational focal point doesn't response within 2 weeks, the request will be elevated to PEPFAR HIS for follow up.

PEPFAR HIS will reach out the PEPFAR Program, the Project Officer and Country Director requesting response and support. If there isn't a response within 2 weeks, access will be deactivated for all users within the organization.

For the validation of each system, the high-level report will be provided to PEPFAR indicating the following:

- Month/ Year of validation;
- Number of Active Users at the beginning of the process;
- Number of Users that were changed to Inactive status at the end of the process by Organization;
- Number of Active users that did not have NDAs by Organization.