

# LINKAGES ACROSS THE CONTINUUM OF HIV SERVICES FOR KEY POPULATIONS AFFECTED BY HIV (LINKAGES)

COOPERATIVE AGREEMENT NO. AID-OAA-A-14-00045

## FACILITATORS' MANUAL ON DATA SAFETY AND SECURITY MEASURES IN THE KEY POPULATION PROGRAM

FHI 360

LINKAGES SRI LANKA

MARCH 2019



*The Facilitators' Manual on Data Safety and Security Measures in the Key Population Program* was developed in Sri Lanka with inputs from the global LINKAGES team.

This document was made possible by the generous support of the American people through the United States Agency for International Development (USAID) and the U.S. President's Emergency Plan for AIDS Relief (PEPFAR). The contents are the responsibility of the LINKAGES project and do not necessarily reflect the views of USAID, PEPFAR, or the United States Government. LINKAGES, a five-year cooperative agreement (AID-OAAA-14-00045), is the largest global project dedicated to key populations. LINKAGES is led by FHI 360 in partnership with InterHealth International, Pact, and the University of North Carolina at Chapel Hill.

## Foreword



The National STD & AIDS Control Program (NSACP) of the Government of Sri Lanka is well positioned to **End AIDS in Sri Lanka** by 2025, ahead of the global target of 2030. For this goal to be achieved, NSACP collaborates with several agencies and partners including - local civil society organizations; communities; United Nations (UN) agencies; and donor organizations including the Global Fund for AIDS, TB and Malaria (GFATM). With GFATM support, the NSACP has been implementing a nation-wide peer-led community outreach program in Sri Lanka in partnership with the Family Planning Association of Sri Lanka, other local CSOs, KP-led organizations and STD clinics. The community outreach interventions cover different

key population groups i.e. female sex workers (FSW), men who have sex with men (MSM), injecting drug user (IDU) and transgender (TG) populations.

Since December 2017, FHI 360, the US-based NGO has been extending technical assistance to NSACP and the local CSO partners to build their technical and program implementation capacity in key population programming. FHI 360 has introduced several global good practices, tools and innovations to address emerging challenges to achieve optimal coverage and HIV testing among different key population groups. This technical assistance is supported by the United States Agency for International Development (USAID) India and USAID Sri Lanka and Maldives Missions as part of a two-year collaborative partnership with the Ministry of Health, Nutrition and Indigenous Medicine (MoH), Government of Sri Lanka.

HIV programs require robust data management to design, implement and monitor programs effectively. Maintaining confidentiality of personal information, their risk level and HIV status are requirements to ensure that there is no harm caused to the key population members. In this regard, FHI 360 helped the CSO partners in Sri Lanka to undertake a self-assessment of their existing data management systems and rate their systems in terms of maintaining data safety and security. Based on the ratings, FHI 360 helped to develop organizational level **Data Safety and Security Policy** and provided orientation to staff. This manual and self-assessment tools helped program managers to improve their existing systems for better data safety and security. All CSO partners working with key population groups have benefitted with these tools.

On behalf of NSACP, I extend my deep appreciation to USAID and FHI 360 for their contribution in developing this guidance document in consultation with local CSOs, seeking technical advice from experts and guidance from FHI 360 global office staff, FPASL, as well my colleagues from NSACP.

Dr. Rasanjalee Hettiarachchi  
Director, National STD & AIDS Control Programme  
Ministry of Health, Nutrition & Indigenous Medicine  
Sri Lanka  
December 2019

## Acknowledgement



FHI 360 has been providing technical assistance in key population programming in the sub-continent for the last two decades working collaboratively with local governments and civil society organizations (CSO) to support innovations at-scale and capacity strengthening in technical and program management areas with a focus on key populations (KP). The United States Agency for International Development (USAID)-funded LINKAGES Project was implemented by FHI 360-led consortium in Sri Lanka from December 2017-December 2019.

We wish to appreciate and acknowledge the leadership, support and guidance extended to FHI 360 LINKAGES Project by Director, National STD & AIDS Control Program (NSACP), Sri Lanka and other members of the senior management team especially Dr. G. Weerasinghe, Senior Consultant-Venereologist and Coordinator-Key Population Program in NSACP, who coordinated the different areas technical assistance seamlessly at the national level. As part of LINKAGES, FHI 360 developed three civil society partners as learning sites for HIV prevention for female sex workers (FSW), men who have sex with men (MSM) and people who use/inject drugs (PWU/ID). The CSO partners adopted tools and technical guidelines in KP programming to enhance coverage and quality of their HIV interventions. Further, their organizational systems were strengthened to improve program delivery at-scale. We acknowledge the leadership and collaborative partnership demonstrated by the three learning site partner organizations namely - Alcohol Drug Information Center (ADIC); Community Strength for Development Foundation (CSDF); and Saviya Development Foundation (SDF). Further, we appreciate and thank contributions made by the community champions and community members, peer educators and field staff, Global Fund for AIDS, Tuberculosis and Malaria (GFATM) supported CSOs implementing KP program in the country, peripheral STD clinics and all those who contributed in adapting the LINKAGES tools and guidelines.

We acknowledge the Ministry of Health (MoH), Government of Sri Lanka and the USAID India and USAID Sri Lanka and Maldives Missions for giving FHI 360 the opportunity to work in Sri Lanka and to contribute towards the national mission of Ending AIDS in Sri Lanka by 2025. FHI 360 received unstinting support and cooperation from other local stakeholders including – GFATM Country Coordination Mechanism (CCM); GFATM local fund agent; UN agencies; Family Planning Association of Sri Lanka. Last but not the least, the FHI 360 teams in headquarters, regional office, India Country Office and the local team of consultants and vendors for their tireless effort and exemplary commitment towards achieving the LINKAGES program results in Sri Lanka.

Dr. Bitra George  
Country Director  
FHI 360 India and Sri Lanka Offices

## Contents

Abbreviations .....	4
<b>1. Introduction</b> .....	<b>5</b>
<b>1.1. Background</b> .....	<b>5</b>
<b>1.2. Training module on data safety and security</b> .....	<b>5</b>
<b>1.3. Agenda of the training</b> .....	<b>6</b>
<b>1.4. Key considerations for successful training</b> .....	<b>7</b>
<b>2. Sessions</b> .....	<b>8</b>
<b>Session I: Introduction of participants</b> .....	<b>8</b>
<b>Session II: Identifying the risks associated with data</b> .....	<b>9</b>
<b>Session III: Preparation to manage data safely and securely</b> .....	<b>12</b>
<b>Session IV: Day-to-day management of paper records</b> .....	<b>16</b>
<b>Session V: Day-to-day management of electronic records</b> .....	<b>21</b>
<b>Session VI: Data sharing and destruction processes</b> .....	<b>26</b>
<b>Session VII: Summing up</b> .....	<b>30</b>
References .....	31

## Abbreviations

CD	Compact disc (media format)
CSO	Civil society organization
DIC	Drop-in center
GFATM	The Global Fund for AIDS, Tuberculosis and Malaria
HIV	Human immunodeficiency virus
IP	Implementing partner
KP	Key population
LGBTI	Lesbian, gay, bisexual, transgender, and intersex
LINKAGES	Linkages across the Continuum of HIV Services for Key Populations Affected by HIV (project)
M&E	Monitoring and evaluation
MEIMS	Monitoring and evaluation information management system
MIS	Monitoring information system
MoH	Ministry of Health, Nutrition and Indigenous Medicine
NGO	Nongovernmental organization
NSACP	National STD/AIDS Control Program
SI	Strategic information
STD	Sexually transmitted disease
ToR	Terms of reference
UIC	Unique identification code
USAID	United States Agency for International Development
USB	Universal Serial Bus (type of storage device)

# 1. Introduction

## 1.1. Background

In Sri Lanka, the key population (KP) program is being implemented by civil society organizations (CSOs). The key components of the prevention program include:

- Registration of KP members and provision of a basic minimum package of services, including behavior change communication and provision of condoms and lubricants (lubes)
- Provision of community-based HIV testing services through drop-in-centers (DICs) and by linking KPs to the nearest sexually transmitted disease (STD) clinics for checking STDs and HIV testing

In the course of providing these services, personal information and sexual health related information is also collected and used for programmatic decision-making. The information is used for estimating the required number of condoms/lubes and monitoring the progress of coverage and testing targets based on service uptake. The program uses unique identification codes (UICs) to register KPs. A mix of paper-based and computer software-based programming is used to manage the information being collected by the program.

The Linkages Across the Continuum of HIV Services for Key Populations Affected by HIV (LINKAGES) project, funded by the United States Agency for International Development (USAID) and implemented by FHI 360, conducted a data security and safety audit using global LINKAGES tools in 2018. The audit was conducted with the three learning site partners who are also implementing the KP program in the country. The exercise identified the following as the areas requiring improvement:

- Improving storage of paper-based and electronic data/records
- Practicing the highest standards of data sharing and data destruction processes
- Ensuring regular internal review and improved practices and procedures to maintain the optimum level of data security and safety standards

## 1.2. Training module on data safety and security

Based on this learning, the LINKAGES project in Sri Lanka developed a one-day training module to train the KP program staff on adopting and implementing the standard processes for data safety and security. The training module comprises:

- A **facilitators' guide** for day-to-day reference as well as for use during the training. It also includes 'ready-to-use' **PowerPoint presentations** (PPTs) and specific session activities to be conducted with trainees. The PPTs will be made available in a USB drive and also uploaded on the National STD/AIDS Control Programme (NSACP) website.
- **Handouts** are also included to provide additional information on each topic and complement the information provided by the facilitator/trainer during the session. It is important for the facilitators to be familiar with the content of the handouts. At the end of the training, each trainee must have a complete set of handouts that they can take back with them for future reference.

As with all training materials, the content of this module must also be revised and updated periodically. It should be reviewed and updated by the trainers before trainings are conducted.

This training manual — *Facilitators’ Manual on Data Safety and Security Measures in the Key Population Program* — has been prepared to assist facilitators in going through the various sessions of the training in a structured manner. Strict adherence to this guide will help achieve the desired goal of promoting robust processes for ensuring data safety and security in the KP program. However, considering the participants’ level of education, knowledge, skills, and expectations, the following flexibilities are acceptable:

- Methodologies can be changed to make the sessions more participatory.
- The duration of different sessions may be altered, but the training should not exceed the total time.

### 1.3. Agenda of the training

Total duration: 6.5 hours Time: Preferably 9 am–5 pm (including 1.5 hours for lunch and tea break)				
Session	Duration	Topic	Activities	Purpose
I	1 hour	Introduction of participants		<ul style="list-style-type: none"> <li>• To build rapport among participants</li> <li>• To ascertain individual expectations from the training</li> <li>• To briefly introduce the training plan</li> </ul>
II	1 hour	Identifying the risks associated with data	Group discussion	<ul style="list-style-type: none"> <li>• To make the participants understand the risks associated with data</li> <li>• To make the participants understand their role in ensuring data safety</li> </ul>
III	1 hour	Preparation to manage data safely and securely	Discussion; presentation	<ul style="list-style-type: none"> <li>• To have the participants prepare a plan to implement data safety and security processes</li> </ul>
IV	1 hour	Day-to-day management of paper records	Group Discussion	<ul style="list-style-type: none"> <li>• To provide information on ensuring that data safety and security standards are maintained for paper records</li> </ul>
V	1.5 hours	Day-to-day management of electronic records	Lab-based activity	<ul style="list-style-type: none"> <li>• To provide information and hands-on practice in managing electronic data, including processes for storage and sharing</li> </ul>
VI	30 minutes	Data sharing and destruction processes	Discussion; presentation	<ul style="list-style-type: none"> <li>• To make the participants aware of the processes for data sharing and destruction</li> </ul>
VII	30 minutes	Summing up		<ul style="list-style-type: none"> <li>• To summarize the learning and highlight the action points</li> </ul>

## 1.4. Key considerations for successful training

- 1) **Ensure that training materials and session outlines are close at hand for easy reference.** This will prevent the use of wrong handouts or case studies during the sessions.
- 2) **Encourage all trainees to be present for the entire training.** In the event of an emergency, in which case a trainee cannot complete the course, the trainer should negotiate with the trainee to complete the missed segments during field trainings or mentoring in the future. Note that this is critical to ensure the quality of training. If a trainee misses any segment of the training, the trainer should brief the trainee about the missed segment when he/she returns.
- 3) **Ensure that the training sessions commence on time.** Request all trainees to arrive on time. Inform them that there is much material to be covered, and it can be disruptive to have trainees arrive while the sessions are underway.
- 4) **Discuss any sensitive issues with the trainees.** It is important for trainers to right at the outset make a statement about any potential discomfort the trainees may feel and invite them to discuss their concerns with the trainer on an individual basis. The group must respect a trainee's decision to pass on a specific question or activity.
- 5) **Encourage trainees to use the question box.** Inform the participants that questions on sensitive issues can be written on a piece of paper and dropped in the question box. The questions should be taken out at the end of the day and discussed in the last session.
- 6) **Encourage trainees to respect individual differences.** Trainees frequently come from different ethnic and cultural backgrounds, and their lifestyles, beliefs, personal experiences, and expertise may differ. The group should respect these differences.
- 7) **Encourage trainees to listen carefully and with empathy, and respect each other's contributions, opinions, and experiences.** Explain that it is important as trainees, and as professionals, to practice active listening by allowing each other to share their own experiences and opinions with the group.
- 8) **Create a congenial environment in which each trainee feels comfortable asking questions.** Trainees should be able to ask questions about what they do not understand. The question box can be a useful tool for this.
- 9) **Ensure the right participants for the training.** Establish clear criteria for participation and communicate the criteria not only to trainees but also to their employers.
- 10) **Ensure that an evaluation form is distributed to trainees at the end of the training.** This form should be completed by each trainee and placed in the 'evaluation box' by the facilitator once all the forms have been submitted.

## 2. Sessions

### Session I: Introduction of participants

Duration: 1 hour

Objectives:

- To build rapport between the facilitator(s) and participants and among the participants
- To list participants' individual expectations from the training

#### Outline: Session I

Step	Content	Time	Method	Materials needed
1	Registration facilitated by the organizer	10 minutes	Individual activity	<ul style="list-style-type: none"> <li>• Registration sheet</li> <li>• Pen</li> <li>• File containing handouts and a copy of the agenda</li> </ul>
2	Welcome address by the organizer	5 minutes	Speech	
3	Introduction and expectation sharing by participants	25 minutes	Activity	<ul style="list-style-type: none"> <li>• 2–3 medium sized plastic balls</li> <li>• 2–3 white chart papers</li> <li>• Post-ads in at least three bright colors</li> </ul>
4	Discussion of the agenda by the facilitator/resource person	10 minutes	Discussion	<ul style="list-style-type: none"> <li>• Copy of the agenda</li> <li>• Projector, projector screen, and laptop</li> </ul>
5	Filling up of the pre-test questionnaire by participants	10 minutes	Individual activity	<ul style="list-style-type: none"> <li>• Copies of the pre-test questionnaire</li> </ul>

#### Session details:

1) Introduction and expectation sharing by participants. (25 minutes)

- Ask the participants to stand in a circle. Give the balls to three participants standing at different points in the circle.
- Explain that in the **first half of the game**, when someone throws the ball to you, you have to say your name and share one 'fun fact' (hobby, food habits, etc.) that describes your personality; e.g., *"My name is Sandeep and I like to chat on Facebook with my friends."*
- Once everyone has said their name, the game is played differently. In the **second half of the game**, when you throw the ball to a person, you have to tell your name and your expectations from the training; e.g., *"This is Nishanka and I would like to learn how to keep data safe."*
- The facilitator(s) must write down the participants' expectations on post-ads and paste them on white chart papers put up on different walls of the hall.
- The facilitator should summarize what the participants are expecting to achieve from the training.

- 2) Brief introduction to the agenda and expected outcomes. (10 minutes)
- The facilitator will present the agenda and help the participants understand the role they will play.
  - The expected outcomes of the training will be shared with the participants.

3) Pre-test questionnaire (10 minutes)

The participants will answer the pre-test questionnaire and submit it to the facilitator.

## Session II: Identifying the risks associated with data

Duration: 1 hour

Objectives:

- To sensitize participants on issues around recording, reporting, and management of data related to the KP program
- To provide an experiential understanding of the situations that expose the data to risk events
- To develop clarity about the role different staff members play in identifying risks in day-to-day handling of KP data and addressing these risks

### Outline: Session II

Step	Content	Time	Method	Materials needed
1	Sharing of personal feelings about the various issues faced by KPs when their data is exposed in the media or to other stakeholders	10 minutes	Individual activity	• Handout A
2	Summary discussion by the resource person	5 minutes	Discussion	
3	Identification of risks in handling KP data and the role of different staff members	20 minutes	Group work (Participants are divided into 3–4 groups, each with representatives from all cadres of staff.)	• Group work instruction sheet (Handout B) • Chart paper, marker pens
4	Presentation by sub-groups	15 minutes	Presentation/ Speech	• Chart paper, marker pens
5	Summary discussion by the facilitator	10 minutes	PPT on summary of the session/ discussion	• Summarize the identified risks and the role of each staff member, as highlighted by participants in the group work

**Session details:**

1) Help the participants to reflect on their views by discussing **Handout A**. (10 minutes)  
Identify the key concerns raised by participants, who they considered responsible for the situation discussed in the handout, and what role they could play in preventing/addressing this situation.

**Handout A: Case study – “A lesson learnt late”**

On a busy afternoon in the summer of 2011, Ramesh, who worked in an NGO, got a call from an unknown number. The caller introduced himself as Charith and said he wanted to come to the NGO’s office to get help. Ramesh provided Charith with all the details and fixed a meeting with him for Monday morning. However, Ramesh forgot to brief his district coordinator and program manager about this meeting. Charith, who worked with a newspaper as a journalist, posed as a gay man seeking care. His motive was to gain access to the LGBTI community group offering HIV services. Charith visited the NGO’s office on Monday and had a long meeting with Ramesh. Ramesh spoke to him about the various activities of the NGO and also shared a few condoms and lubes that the NGO’s outreach workers provide to KPs. A few days later, Charith published an exposé on condom and lube distribution to gay men, naming the NGO and providing its address. As a result of the newspaper article and the public response, several NGOs, including Ramesh’s, had to stop operations and many others had to shut down their websites and Facebook pages.

2) Discuss the points given below and summarize. (5 minutes)

- Identify the risks associated with the information shared by Ramesh (refer to Handout A).
- Discuss Ramesh’s expected role in such situations.

3) Organize group work. (20 minutes)

Tell the participants they will take part in group work, where they will identify risks to KP data and the role various staff members can play.

Divide the participants into 3–4 sub-groups, each with representatives of the various cadres of staff, including those responsible for data collection, data recording and reporting, and use of data for day-to-day management of the program.

Share the group work discussion guide (**Handout B**). Each sub-group is expected to discuss and present the points on the provided chart paper.

**Handout B: Group Work Discussion Guide**

Name of the MIS/data collection formats used by the program	Format (Indicate ‘P’ for paper format, ‘E’ for electronic records, and ‘M’ for both paper and electronic formats)	Purpose of use (‘C’ for collection, ‘R’ recording only, ‘S’ for reporting only)	Frequency of use (‘D’ for daily, ‘W’ for weekly, ‘F’ for fortnightly, ‘M’ for monthly, and ‘Q’ for quarterly)	Person responsible for use of the MIS/data collection format	Report any risk events experienced for the particular MIS/data collection forms in the last one year	Action taken to address the risk event	Recommended solution to prevent such risk events

4) Facilitate the sub-groups in presenting their ideas. (15 minutes)

Use the following table to summarize the key risk areas identified by the sub-groups for each of the MIS/data collection formats. The table below is populated with some responses.

<b>MIS/data collection format</b>	<b>Risk levels</b>	<b>Person(s) responsible</b>	<b>Solutions recommended</b>
<b>Peer registration sheet</b>	High (because personal information is recorded)	<ul style="list-style-type: none"> <li>• Peer educator</li> <li>• Field supervisor</li> <li>• M&amp;E officer</li> </ul>	The complete information on a KP should be collected in multiple phases of registration (Phase 1: Name and contact details; Phase 2: Information on sexual health; Phase 3: Risk behavior, etc.)
<b>Peer diary</b>	High (because it is used daily and has details of interactions)	<ul style="list-style-type: none"> <li>• Peer educator</li> <li>• Field supervisor</li> <li>• M&amp;E officer</li> </ul>	<ul style="list-style-type: none"> <li>• Peer records need to be managed in a safe manner. No records should be kept at the peer educator's home or workplace for more than a week. Records should be submitted to the office on a weekly basis.</li> <li>• The peer educator should maintain minimum records.</li> </ul>
<b>Condom and lube distribution register</b>	High (because it is linked with personal information and sexual health information)	<ul style="list-style-type: none"> <li>• Peer educator</li> <li>• Field supervisor</li> </ul>	<ul style="list-style-type: none"> <li>• Maps and pictorial tools that do not directly show condom/lube distribution or risk information may be used for recording and reporting purposes.</li> <li>• The data from the peer diary should be stored at the organization's office and electronically maintained in the required formats.</li> </ul>
<b>HIV escort referral information</b>	Moderate (because it is linked with personal information)	<ul style="list-style-type: none"> <li>• Peer educator</li> <li>• Field supervisor</li> </ul>	<ul style="list-style-type: none"> <li>• Escort slips should be kept at the organization's office. Cross-checking should be done by the field supervisor only.</li> </ul>
<b>HIV escort slips</b>	Low (because the information is encrypted and linked to clinic visits)	<ul style="list-style-type: none"> <li>• Field supervisor</li> </ul>	<ul style="list-style-type: none"> <li>• Escort slips can be barcoded and maintained at the organization's office.</li> <li>• Barcoded slips can be handled for cross-checking at the clinic.</li> </ul>
<b>Pocket meeting reports</b>	Low (because the information is related to community meetings)	<ul style="list-style-type: none"> <li>• Peer educator</li> <li>• Field supervisor</li> </ul>	<ul style="list-style-type: none"> <li>• Signatures of the participants can be cross-checked with registration sheets and use of name avoided.</li> </ul>
<b>MEIMS reporting platform</b>	Moderate (because the information is maintained in a secure server and personal information is encrypted as UICs)	<ul style="list-style-type: none"> <li>• M&amp;E officer</li> </ul>	<ul style="list-style-type: none"> <li>• Passwords and user access control should be maintained.</li> <li>• In case the data is downloaded for programmatic use, names and contact details of KPs should be used in a very restricted manner.</li> <li>• No hard copy of the registration or service details should be shared without necessary prior approval.</li> </ul>

			<ul style="list-style-type: none"> <li>• Excel datasheet should be shared only with password.</li> </ul>
<b>Quarterly summary report</b>	Low (because aggregated data is used for reporting)	<ul style="list-style-type: none"> <li>• M&amp;E officer</li> </ul>	<ul style="list-style-type: none"> <li>• Quarterly report should be shared with the designated authority only.</li> <li>• In case individualized data is shared, it should be encrypted.</li> </ul>

5) Discuss the recommendations with participants and build consensus in terms of their role and responsibilities. (10 minutes)

Summarize the key takeaways from the session, as listed below.

Key takeaways:

- Each staff member has a role in ensuring that the information/data they collect is in safe hands and securely handled.
- Only the information that the program needs should be collected and not what will never be used by the program.
- Breach in an individual's confidentiality can lead to blackmail, physical and/or sexual violence, job loss, loss of custody of children, and widespread marginalization.
- Breach in data safety can lead to loss of trust in healthcare services or the program, which will negatively affect service uptake.
- Breach in data safety can harm implementers/service providers, who may be targeted for their possible involvement.
- Failure to protect data can render a project unable to provide appropriate services or report on activities.

### Session III: Preparation to manage data safely and securely

Duration: 1 hour

Objectives:

- To provide an experiential understanding of the current practices in data storage
- To build knowledge on the standard processes to be used in storing data in future

**Outline: Session III**

Step	Content	Time	Method	Materials needed
1	Existing practices	20 minutes	Group work – Draw your store	<ul style="list-style-type: none"> <li>• Flip chart and marker pens (The number of flip charts will depend on the number of sub-groups.)</li> </ul>
2	Summary discussion	10 minutes	Discussion/PPT on the summary of existing practices	<ul style="list-style-type: none"> <li>• Flip chart and marker pens</li> </ul>
3	Standard practices for safe and secure management of data	30 minutes	PPT on standard practices/discussion	<ul style="list-style-type: none"> <li>• Projector, projector screen, and handout</li> <li>• Flip chart</li> </ul>

**Session details:**

1) Discuss the existing practices related to data storage. (20 minutes)

Ask the participants (in the same sub-group composition as the last group work) to re-assemble near the flip charts put up for each sub-group. Ask the participants to think about and draw pictures (not artistic but accurately representative) of their day-to-day practices for the following:

a) For storing paper-based records that they carry home or to the place where they work (especially for peer educators and field supervisors). Some possible responses are presented below:

- i. Lying on the dining table at home
- ii. Inside a bag that is carelessly left around the house/workplace

Ask the participants to think about and note the benefits and concerns with such practices.

Benefits	Concerns
•	•

b) For storing paper-based records at office; some possible responses are presented below:

- i. Lying in heaps at the M&E officer’s desk
- ii. Lying inside a carton in the storeroom or in a box near the toilet
- iii. Lying scattered on a table

Ask the participants to think about and note the benefits and concerns with such practices.

Benefits	Concerns
•	•

c) For storing electronic records at office; some possible responses are presented below:

- i. On the laptop without any password
- ii. On the office pen-drive, along with other data and favorite songs and movie files
- iii. On an Excel sheet without any password protection
- iv. On registration sheets filled with personal details of KPs

Ask the participants to think about and note the benefits and concerns with such practices.

Benefits	Concerns
•	•

2) Summarize the discussion. (10 minutes)

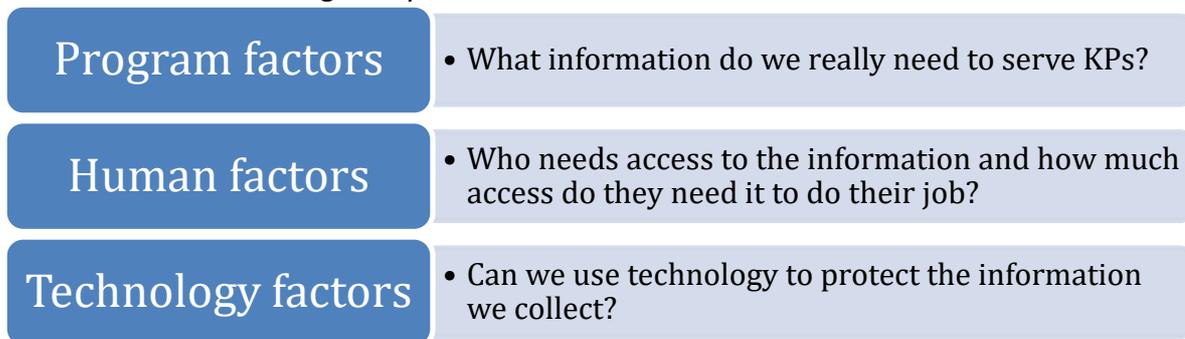
Ask the sub-groups to move in a clockwise direction and spend two minutes studying the flip charts prepared by other sub-groups. Tell them to write down any points they feel are missing and need to be mentioned on the flip chart. Once each sub-group has completed looking at the flip charts prepared by other sub-groups, summarize your observations, as listed below.

- Gaps in safekeeping of records can lead to misuse of information, violence toward the organization’s staff and their colleagues/family members, and closure of the project, which will deprive KPs of the services they receive through the project.
- Gaps in safekeeping of records at home/workplace or at the project office may lead to loss of information and exposure of KP members, causing them to lose trust in the program and the organization.

- Gaps in safekeeping of records may lead to disturbances in the KPs' family, especially if family members come to know that the project is working with sexual minorities, drug users, and FSWs and distributing condoms/lubes to KPs.
- Gaps in safekeeping of records may lead to loss of records partially or completely, thereby hampering quality of reporting and service delivery.

**Figure 1: Risks and benefits - What is the balance?**

It is important to collect data, but the data can end up hurting the KPs. The risks and benefits need to be thoughtfully considered.



3) Share the standard practices for safe and secure management of data. (30 minutes)

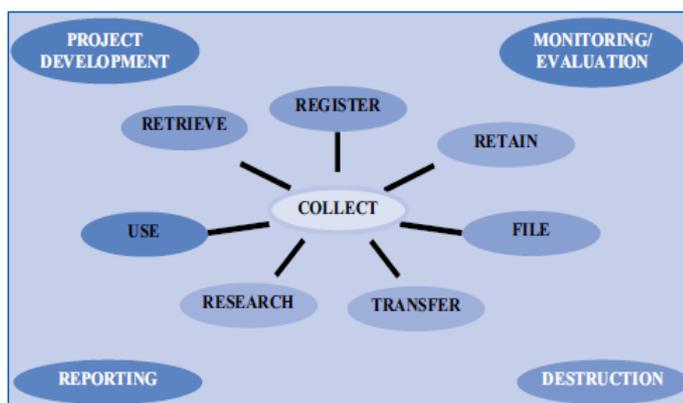


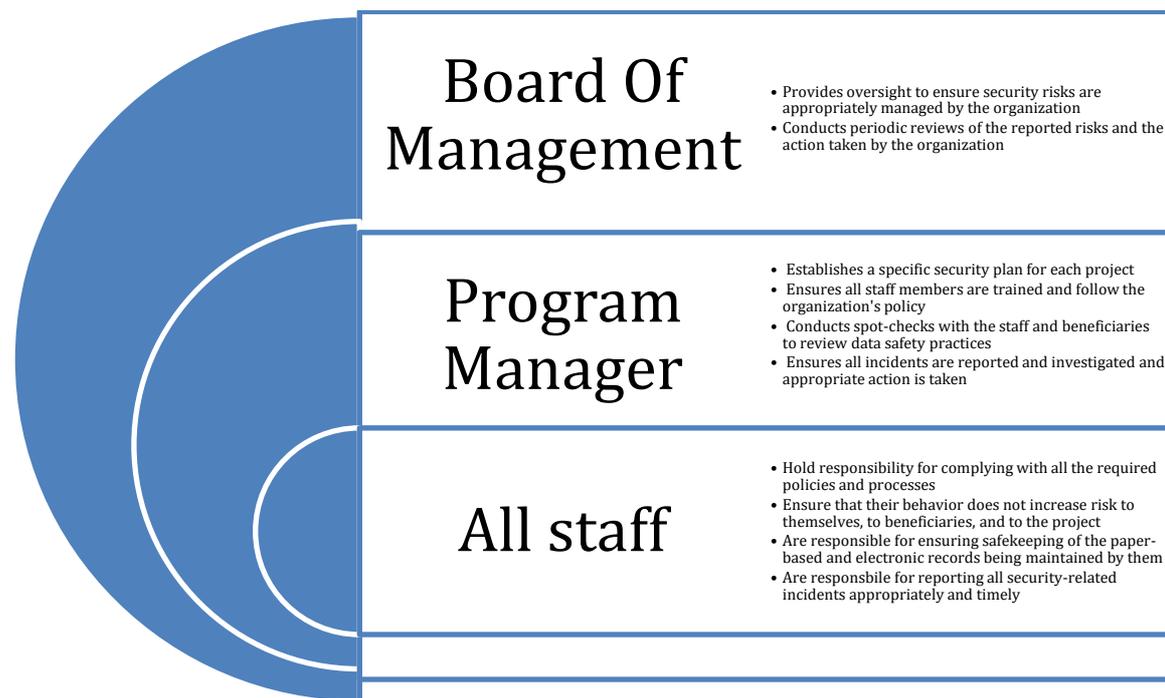
Figure 2 shows the different phases of data processing, and that everyone in the team is responsible for these processes.

**Figure 2: Data processing activities** (Source: IOM Data Protection Manual)

To manage the activities mentioned in Figure 2, each member of the team needs to perform specific roles and responsibilities and abide by the organization's policy on data safety and security. These aspects are discussed in a step-by-step manner below.

## Step 1: Understanding role and responsibilities

Figure 3: Roles and responsibilities within the organization



## Step 2: Development of the organization's data safety and security policy

A data security policy is a must for all organizations, irrespective of size. This policy informs the staff about the principles, approaches, and responsibilities related to data security and risk management and ensures that staff act in a manner that is appropriate for the organization.

The data safety and security policy should be a short and accessible document that is translated into the organization's core operational languages. Most such policies are structured around four key sections:

1. A statement on the importance of the staff's responsibility to ensure data security and safety, the scope of the policy, and who it applies to.
2. A section defining the principles that underlie the organization's data safety and security culture — respecting each individual's identity and how they expect to participate in the program; highlighting every staff member's shared responsibility of managing and reducing data security risks; not requiring the staff to ever put themselves at excessive risk in order to meet the program's outcomes; recognizing that some staff members/volunteers are more at risk than others due to the nature of their work and must be informed and equipped with solutions; understanding the need to withdraw from a particular location if the situation poses a threat to continued service provision and maintaining the safety of records/data. This section should also explain the organization's risk attitude and its commitment to handling each risk with utmost attention and effort and addressing it through solutions that do not compromise any beneficiary's right to privacy. It should also explain the key principles that shape the organization's existing systems for data security and safety.
3. A section on roles and responsibilities, setting out the organization's risk management structure and the roles and tasks allocated to each position/cadre.

4. A section detailing the minimum security requirements. This section establishes the specific organizational requirements that must be in place; e.g., the organization must have a safety and security plan for each project and the concerned staff should have been oriented on it.

All organizations are required to establish a data safety and security policy and standard operating procedures (SoPs). All the concerned staff must be oriented on these from time to time during ongoing project activities.

Summarize the discussion through the key takeaways mentioned below.

Key takeaways:

- Organizational policy and standard processes are essential to ensure that any safety and security risks are identified timely and appropriate actions are taken by the concerned staff.
- Data safety and security standards are guided by the nature of information being collected, recorded, reported, and used by the program.
- Each staff member has a role to play in ensuring that data safety and security standards are implemented in true spirit.

### Session IV: Day-to-day management of paper records

Duration: 1 hour

Objectives:

- To introduce the concept of day-to-day management of paper records
- To build knowledge on the various steps to be taken by the organization to ensure that data safety and security standards are maintained for paper records

**Outline: Session IV**

Step	Content	Time	Method	Materials needed
1	Need for safety and security of paper records	20 minutes	Discussion of the case study	<ul style="list-style-type: none"> <li>• Projector, projector screen, and Handout C</li> <li>• Flip chart</li> </ul>
2	Steps to ensure data safety and security standards for paper records	40 minutes	PPT on the steps for maintaining paper records/ discussion	<ul style="list-style-type: none"> <li>• Handout D</li> <li>• Handout E</li> <li>• Flip chart</li> <li>• Projector and screen</li> </ul>

**Session details:**

1) Discuss the need for safety and security of paper records. (20 minutes)

Provide **Handout C** and discuss the case study with participants. Encourage them to respond to the following questions:

- I. What went wrong in this scenario?
- II. Who was responsible for this situation?
- III. What action would they have taken in such a situation?

### **Handout C: Case Study – “Oops moments with our data”**

Shakthi has been working as a peer educator with female sex workers (FSWs) for the last four years. She is a diligent worker, and every FSW feels empowered when she speaks to Shakthi. The NGO recently awarded Shakthi for being the most honest and hardworking peer educator. In addition to working as a peer educator, she also works at a spa part time, which earns her a handsome salary. Last Wednesday one of her clients sent her an SMS with a picture of a page from her peer educator diary, in which details of the condoms distributed to fellow FSWs were mentioned. Shakthi deleted the message and asked the client to not circulate the picture because it may jeopardize the work she does for HIV prevention among FSWs. The client blackmailed her and asked for LKR 2,000 in return for not circulating the picture. Shakthi paid LKR 2,000 to ensure that her reputation is not at stake. On Friday, the organization received a phone call from a man asking how many sex workers they worked with in the locality. The staff member who received the phone call was shocked and asked the caller why such information was required and asked him to leave his contact details for a call back later. The caller’s contact details were noted, and on further investigation it was found that the man was known to Shakthi. The project officer called for an urgent meeting with the staff. At the meeting, Shakthi disclosed the entire series of event. She also informed the team that she used to carry her peer educator diary to the spa where she works and often shares the contact details of other FSWs with clients to earn a commission from them. She also mentioned that she often clicks pictures of her peer educator diary to conveniently share contact details of other FSWs with clients over WhatsApp.

2) Explain the steps to ensure data safety and security standards for paper records. (40 minutes)

To protect service users’ (beneficiaries’) data, implementer safety, and programmatic integrity, the LINKAGES Global Strategic Information Team has developed a checklist (Data Safety Checklist) of actions that should be taken by implementing partners (IPs) collecting, managing, analyzing, and storing paper data. The IPs and strategic information (SI) backstops should use the checklist and provide detailed guidance on implementation to ensure that adequate protective measures are in place. The checklist is provided in **Handout D**.

**Handout D: Data Safety and Security Checklist** (Source: LINKAGES tools for Data Safety and Security Assessment)

DATA SAFETY AND SECURITY CHECKLIST			
Assessment Categories/Items	Means of verification	Answer	Comments
<b>PAPER RECORDS</b>			
1. Have a list of all documents requiring safe storage (i.e., all documents containing information that can be used to identify individual KP members)	Staff Interview	No	
2. Have established a space for safe storage, such as a locked safe or cabinet, where paper records with individual identifying information is	Staff Interview	Yes	
3. Access to this safe storage is controlled by selected staff and tracked	Staff Interview	Yes	
4. Have created a list of staff responsible for moving data to safe storage, including periodicity and specific procedures or protocol for handling individual records	Staff Interview	No	
<b>ELECTRONIC DATA SYSTEMS</b>			
5. All databases are password protected	Staff Interview	No	
6. Access to passwords for databases and electronic data is controlled	Staff Interview	No	
6. Use of UICs when possible to identify individuals	Staff Interview	Yes	
8. Electronic data is securely backed-up and stored either in Cloud and/or on flash drive in remote location	Staff Interview	Yes	
9. Have a protocol for changing password when staff depart	Staff Interview	Partially	
<b>DATA SHARING AND DESTRUCTION PROCEDURES</b>			
10. Have protocols/guidelines for sharing data with other partners	Staff Interview	Partially	
11. List of individual(s) with right to destroy data (e.g., in case of pending police raid)	Staff Interview	No	
12. Protocol for safe data destruction of records	Staff Interview	No	
<b>STAFF TRAINING AND MANAGEMENT</b>			
13. Employees were trained in data confidentiality within the past year	Staff Interview	Yes	
14. Protocols in place to guide action in case of individuals who may have intentionally violated data confidentiality regulations	Staff Interview	Partially	

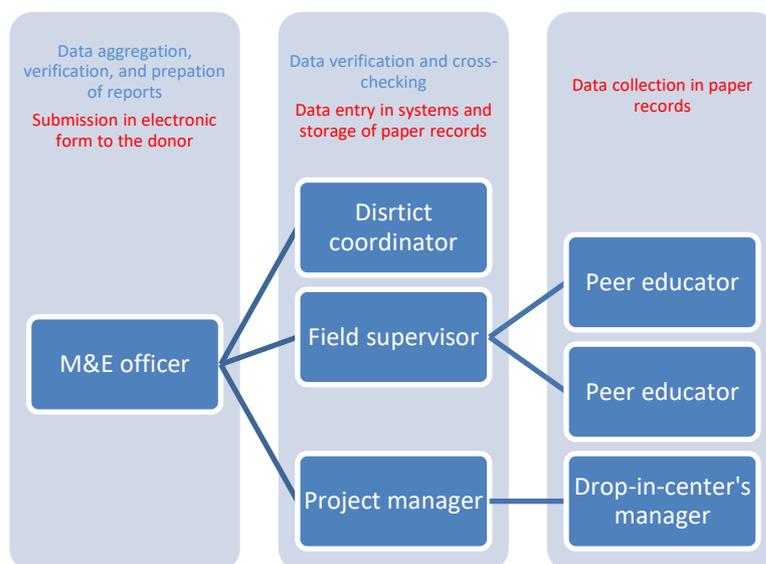
Ask the participants to use the Data Safety Checklist (Handout D) to assess ongoing practices continuously, preferably at the start of any project and every six months thereafter. This can be the self-reported checklist for the M&E and program teams to assess the potential risks and existing practices. It will help them identify the steps to be taken to improve the data safety standards outlined in the policy.

In the table below, the left column includes the checklist items along with additional information on how to operationalize these items. The right column includes example documents (or elements of such documents) that will support operationalization. It also includes illustrative examples in italics to help populate these documents. The illustrative examples are meant only to help the IPs think about the content of the documents and are not prescriptive.

Instructions	Documents to support operationalization (with illustrative examples)
<p>1. Make a list of all the documents that require safe storage (i.e., all the documents containing information that can be used to identify individual KP members).</p> <ul style="list-style-type: none"> <li>• Update the list of documents each quarter when developing quarterly reports (in the process you may realize that you are using new documents that also contain identifying information).</li> <li>• The list should include anything that contains individual level data and personal information about a service user.</li> </ul>	<p>List of documents requiring safe storage and date of last review</p> <ul style="list-style-type: none"> <li>• <i>KP registration forms</i></li> <li>• <i>Peer educator diary</i></li> <li>• <i>Condom distribution registers</i></li> <li>• <i>Clinic escort slips</i></li> <li>• <i>Sign-in sheets</i></li> <li>• <i>Clinical records</i></li> <li>• <i>Outreach logs/travel documents</i></li> <li>• <i>Individual tracking data being used for microplanning</i></li> <li>• <i>Date of last review</i></li> </ul>
<p>2. Establish a safe storage space, such as a locked safe or cabinet where paper records with individual identifying information can be stored.</p> <ul style="list-style-type: none"> <li>• The storage space should be easily identifiable and accessible during a site visit. If audited through a visit, the location should be checked to ensure that it is locked and the key cannot be easily located.</li> <li>• There should be a mechanism in place to ensure that duplicate keys cannot be made.</li> </ul>	<p>Description of safe storage location and the protections in place</p> <ul style="list-style-type: none"> <li>• <i>File cabinet with lock</i></li> <li>• <i>Only select staff should have access to the key, which cannot be duplicated</i></li> </ul>
<p>3. Ensure that access to the safe storage space is controlled by selected staff and tracked.</p> <ul style="list-style-type: none"> <li>• A list of staff members who can access the safely stored documents should be kept with the list of documents requiring safe storage. The list should be updated whenever a staff member who has access stops working for the IP for any reason; the list should be reviewed quarterly.</li> <li>• Each time a staff member with access leaves the organization, the code (if a combination) should be changed and the keys all accounted for or locks changed.</li> <li>• Someone occupying a higher level position with a relatively low turnover, such as the organization's director, should be the final person responsible for data</li> </ul>	<p>Names of staff members with access to paper-based data and date of last review</p> <ul style="list-style-type: none"> <li>• <i>Staff name, date the access began, date the access ended</i></li> <li>• <i>Date of last review</i></li> </ul> <p>Name of the data safety point of contact</p>

Instructions	Documents to support operationalization (with illustrative examples)
<p>safety. He/she should be referred to as the 'data safety point of contact' and must be aware of and sign-off when any changes are made. The data safety point of contact will also need to be trained (see point 4 below).</p> <ul style="list-style-type: none"> <li>Keep a logbook to track persons who have accessed the safe storage location at any time.</li> </ul>	<p>Logbook to track access to the safe storage location</p>
<p>4. Create a list of staff members responsible for moving data to the safe storage space, including the periodicity and specific procedures or protocol for handling individual records.</p> <ul style="list-style-type: none"> <li>Create an easy-to-use graphic that depicts data movement (e.g., from peer educators to data entry personnel) and names of each individual and their position; this is part of the protocol for safe handling of individual records.</li> <li>Have job descriptions for positions that entail data handling, including specific responsibilities around data storage and record handling and a confidentiality clause.</li> <li>A confidentiality statement/agreement should be signed by all those named as having access to identifiable data, both paper- and electronic-based. Example of a confidentiality statement can be found in the <a href="#">Program Monitoring Guide</a> (pg. 22). The signed statements must be safely stored so that they can be referred to as needed.</li> <li>The staff members responsible for data entry (i.e., when paper-based data is entered into electronic format), such as an M&amp;E officer, should also be named and made to sign the confidentiality statement.</li> </ul>	<p>Graphic describing how data moves</p> <p>List of job descriptions for positions that entail access to data storage and handling of records</p> <ul style="list-style-type: none"> <li><i>Peer educator</i></li> <li><i>Field supervisor</i></li> <li><i>District coordinator</i></li> <li><i>DIC manager</i></li> <li><i>M&amp;E officer</i></li> </ul> <p>List of staff members responsible for moving data, along with the date on which each person signed the confidentiality statement</p>

Figure 4. Data movement diagram created by a CSO implementing the KP program in Sri Lanka



As seen in Figure 4, all the staff members have a specific role to play at different stages and should be aware of their responsibilities for maintaining data safety and security. Their terms of reference (ToRs) need to have details of their responsibilities and the reporting requirements for ensuring data security risks are reported timely. Also, each of them should sign the confidentiality agreement; example of a confidentiality agreement is provided in **Handout E**.

### **Handout E: Example of a Confidentiality Statement/Agreement**

*(Source: Monitoring Guide and Toolkit for Key Population HIV Prevention, Care, and Treatment Programs)*

**OATH OF CONFIDENTIALITY**

I understand that, in the course of my duties in this service, I will come in contact with sensitive, personal information about individuals who would agree to be part of the intervention. I understand that this information is highly confidential, and I pledge to protect the confidentiality of all individuals attending the service. I will protect the confidentiality of patients by not discussing or disclosing any information about them to an unauthorized person, including the fact that they attended these services. Unauthorized persons may include, but are not limited to, my family, friends, co-workers and community leaders. I understand the potential social harm that may come to patients whose personal and medical information is disclosed to unauthorized persons.

I understand that willful disclosure of any information about any key population member in this program could result in termination of my employment or result in legal action against me.

Signature of staff member: \_\_\_\_\_ Witness: \_\_\_\_\_

Date: \_\_\_\_\_

Summarize the discussion through the key takeaways mentioned below.

#### Key takeaways:

- Paper records with individual/personal information of KP members are required to be kept in safe storage under lock and key.
- The safe storage space and each movement of records should be tracked in a logbook, with names of the staff members who handled the records and the time and date the records were accessed.
- A quarterly review of the processes and logbook should be undertaken. In case new paper records are added to the project, the list in the logbook should be updated.
- Each staff member should be provided details about their responsibilities to ensure data safety and security. These details should be mentioned in their ToRs/job descriptions and they should be made to sign a confidentiality agreement.

## **Session V: Day-to-day management of electronic records**

Duration: 1.5 hours

#### **Objectives:**

- To introduce the concept of day-to-day management of electronic records
- To build knowledge on the various steps to be taken by the organization to ensure data safety and security standards are maintained for electronic records

**Outline: Session V**

<b>Step</b>	<b>Content</b>	<b>Time</b>	<b>Method</b>	<b>Materials needed</b>
1	Need for safety and security of electronic records	20 minutes	PPT on the steps for maintaining electronic records; discussion on the given scenarios	<ul style="list-style-type: none"> <li>• Projector, projector screen</li> <li>• Flip chart</li> </ul>
2	Steps to ensure data safety and security standards for electronic records	60 minutes	PPT on the steps for maintaining electronic records/ discussion	<ul style="list-style-type: none"> <li>• Participants’ laptops</li> <li>• Dummy data sheets</li> <li>• Flip chart</li> <li>• Projector and screen</li> <li>• Handout D</li> </ul>
3	Summary discussion	10 minutes	Discussion	<ul style="list-style-type: none"> <li>• Flip Chart and marker pens</li> </ul>

**Session details:**

1) Discuss the need for data safety and security practices for electronic records. (20 minutes)

Start the discussion with the following questions and list the responses on a flip chart. The questions to be discussed are:

- Do the desktops, laptops, mobile, and tablet devices we use for program purposes have an updated anti-virus and are in good operating conditions?
- Have we ever experienced loss of data due to malfunctioning gadgets or loss of gadgets?
- Have we ever experienced someone stealing our data or changing our data when we shared the data through a USB drive or over e-mail?
- Have we ever connected to an open Wi-Fi network just for a fun and also used it for official purposes?
- Do we share our passwords within the team and outside the team?
- How often do we change our passwords? When did we last change our passwords?

Summarize the discussion by emphasizing the need for greater care and for continuous efforts to ensure that electronic data is kept safe and secure.

2) Explain the steps to ensure data safety and security standards for electronic records. (60 minutes)

To protect service users’ data, implementer safety, and programmatic integrity, the LINKAGES Global Strategic Information Team has developed a checklist (Data Safety Checklist) of actions that should be taken by implementing partners (IPs) collecting, managing, analyzing, and storing electronic data. The IPs and strategic information (SI) backstops should use that checklist and provide detailed guidance on implementation to ensure that adequate protective measures are in place. The checklist is provided in **Handout D**.

Ask the participants to use the Data Safety Checklist (Handout D) to assess the current practices continuously, preferably at the start of any project and every six months thereafter. This can be the self-reported checklist for the M&E and program teams to assess the potential risks and existing practices. It will help them identify the steps that need to be taken to improve the data safety standards outlined in the policy.

In the table below, the left column includes the checklist items from the Data Safety Checklist along with additional information on how to operationalize these items. The right column includes examples of documents (or elements of such documents) that will support operationalization. It also includes illustrative examples in italics to help populate these documents. The illustrative examples are meant only to help the IPs think about the content of the documents and are not prescriptive.

<b>Instructions</b>	<b>Documents to support operationalization (with illustrative examples)</b>
<p>1. Ensure all databases are password protected.</p> <ul style="list-style-type: none"> <li>• Computers require passwords to open them. Databases should require an additional, separate password. Ideally, there should also be a password for administrative access, which should be separate from the user password.</li> <li>• A strong password is around 10 characters long or more. Where possible, include uppercase letters, lowercase letters, numbers, and symbols in the password. Do not write down a password or share it.</li> <li>• Passwords should be changed every three months. Passwords may need to be changed sooner if security has been compromised or a staff member has left the organization.</li> <li>• Systems to prevent sharing of passwords should be in place (e.g., two persons should not have the same log-in credentials).</li> </ul>	<p>A log to track that all computers and databases have passwords</p> <p>Record of the date when passwords were last changed for the computers where data is stored</p> <p>Record of the date when passwords were last changed for databases</p>
<p>2. Control access to passwords for databases and electronic data.</p> <ul style="list-style-type: none"> <li>• Any data containing individual identifying information must be stored in a password-protected file, including when it is sent over e-mail or uploaded on cloud.</li> <li>• There should be proper listing of which staff member(s) can access the database to enter data and to see the full database. Two different passwords should be in place, one for data entry and the other for access to the full database.</li> </ul>	<p>Names of staff members with access to electronic data and the dates when access began and ended</p>
<p>3. Use UICs when possible to identify individual KPs.</p> <ul style="list-style-type: none"> <li>• Follow the UIC guide recommended by NSACP, Sri Lanka.</li> </ul>	<p>UIC generation guidance</p>
<p>4. Ensure electronic data is securely backed-up and stored either in cloud and/or on a drive in a remote location.</p>	<p>Describe back-up</p> <ul style="list-style-type: none"> <li>• <i>Cloud</i></li> <li>• <i>USB drive</i></li> </ul>

<ul style="list-style-type: none"> <li>• The IP should decide on whether to use cloud or local storage based on local guidance from the government and the cost of cloud storage (which depends on the size of data to be stored).</li> <li>• Safe cloud storage requires a password. If possible, use an encrypted storage platform such as Google Drive.</li> <li>• The remote drive (e.g., a CD or a USB drive) should also be password protected and its location known only to those who have access to the full database.</li> <li>• Data back-up should be done weekly.</li> <li>• Protections for the backed-up data should be clearly described.</li> </ul>	<ul style="list-style-type: none"> <li>• <i>CD</i></li> <li>• <i>Date of last backup</i></li> </ul> <p>Describe data protection measures</p> <ul style="list-style-type: none"> <li>• <i>Password</i></li> <li>• <i>Encryption</i></li> <li>• <i>Safe location of hard drive</i></li> </ul>
<p>5. Have a protocol for changing password(s) when a staff member leaves the organization.</p> <ul style="list-style-type: none"> <li>• Each time a staff member with data access leaves the organization, the password must be immediately changed. If a staff member is being terminated, the password should be changed before the decision to terminate is communicated to him/her.</li> <li>• If a staff member is changing positions within the organization and will no longer have access to the database, the password must be changed immediately.</li> </ul>	<p><i>Whenever a staff member, consultant, or another individual with access to the stored data or the ability to enter data is terminated or leaves the organization, his/her access should also be terminated. If he/she has a log-in name, it needs to be deleted. In case the person is being terminated, his/her access to data should be blocked before the decision to terminate is communicated to him/her.</i></p>

Discuss the case scenarios given below and help the participants in hands-on practice on their laptops/desktops. The hands-on training is on creating and changing passwords and on handling unsolicited attachments received over e-mail.

### Scenarios for Hands-on Practice

Scenario 1	Discussion points	Exercise for hands-on practice
<p>Kumar has important data on a USB drive, which he used from home last night. When he plugged the USB into the office desktop, some of his folders and files were not visible. He was confident that the files he worked on last night were in the USB drive. He checked the USB drive on his personal</p>	<p>What could be the potential issue Kumar has faced?</p> <p><i>He is most likely experiencing malware infection on the office desktop. Malware is a threatening software that can affect all computer users. Malware can lead to information loss, reduced performance, theft of documents, and spying.</i></p>	<ul style="list-style-type: none"> <li>• If you find malware on your computer, unplug your computer from the Internet and stop using it immediately.</li> <li>• You may wish to take your computer to a security expert, who may be able to discover more details about the malware.</li> <li>• Use another system you believe is safe and change your passwords; every password that you had typed on your computer while it was infected may now stand compromised.</li> </ul>

<p>laptop at home; the files and folders were working there.</p>	<p>Malware is the short form of the term ‘malicious software’ and is intended to allow an attacker to record from a webcam and microphone, disable the notification settings for anti-virus programs, record keyboard strokes, copy e-mails and other documents, steal passwords, and more.</p>	<ul style="list-style-type: none"> <li>• <b>Use Flexera PSI over the Internet. This will help to check your installed software and version numbers against an online database of current version numbers and link you to download new versions of your programs.</b></li> </ul>
<p><b>Scenario 2</b></p>	<p><b>Discussion points</b></p>	<p><b>Exercise for hands-on practice</b></p>
<p>In the morning, Kumar received an e-mail with an attachment on his Gmail account. He was happy to see the information and downloaded the attachment. Suddenly his laptop blinked and restarted on its own. Kumar thought this is normal.</p>	<p>What do you think are the possible reasons?</p> <p><i>The file attachment in the e-mail may be a virus or malware that has impacted Kumar’s system.</i></p>	<p>Let us learn how to use Gmail effectively. If you are using Gmail, you can view the attached document by clicking on this square (and not the download arrow). It will appear in your browser through Google’s filters rather than downloading and opening on your computer, thereby protecting you from any risks the attachment may pose.</p> 
<p><b>Scenario 3</b></p>	<p><b>Discussion points</b></p>	<p><b>Exercise for hands-on practice</b></p>
<p>Kumar got a new desktop recently. He wants to set up the same password as the one he used for the computer he was using for the last few years.</p>	<p>Is Kumar doing the right thing?</p>	<ul style="list-style-type: none"> <li>• There are a few passwords that need to be particularly strong and need to be memorized (not written down). These are the passwords you must use to lock your data safely. These include, at least, the passwords for your computer system and e-mail accounts.</li> <li>• A combination of alphabets, numbers, and special characters should be used to make a strong password. Your password should not contain your name, date of birth, phone number, pin code, vehicle registration number, etc.</li> <li>• Google mail accounts come with multi-factor authentication, which prompts the user to allow permission over their phone if someone accesses their Google account. An updated list of these services is available at: <a href="https://www.turnon2fa.com">https://www.turnon2fa.com</a>.</li> <li>• Another way of managing passwords is to use a password manager software like KeePassX. It is an open source and free password vault that you can keep on your desktop. Note that if you are using KeePassX, it will not automatically save changes and additions. This means that if it crashes after you added some passwords, you can lose them forever.</li> </ul>

		<p>However, you can change this in settings. Using a password manager will also help you to choose strong passwords that are hard for an attacker to guess.</p> <ul style="list-style-type: none"> <li>• Lastly, keep a log of passwords under lock and key, with a mention of the dates when these were changed and who made the change.</li> </ul>
--	--	--

### 3) Summarize the discussion. (10 minutes)

Highlighting the need for ensuring the following:

- Use of UICs for records with personal information
- Maintaining passwords for e-mail accounts and Excel sheets with sensitive data
- Avoiding, unless necessary, the use of the official e-mail account or USB drive in public places/on open Wi-Fi
- Keeping a log of passwords for all e-mail accounts and electronic records under lock and key

End the discussion by highlighting the key takeaways mentioned below.

#### Key takeaways:

- In today's world, electronic records are increasingly being used by all of us. It is our duty and responsibility to ensure the safety and security of such records.
- The policy for maintaining safety and security of data should be adhered to by all staff members. It should also be informed to all the stakeholders while developing M&E systems and sharing information electronically.

## Session VI: Data sharing and destruction processes

Duration: 30 minutes

Objectives:

- To help the participants understand the need for safe and secure data sharing processes and the requirements for data destruction

#### **Outline: Session VI**

Step	Content	Time	Method	Materials needed
1	Processes for data sharing	20 minutes	Presentation/discussion	<ul style="list-style-type: none"> <li>• Flip chart, marker pens</li> <li>• Handout D</li> </ul>
2	Data destruction processes	10 minutes	Presentation/discussion	<ul style="list-style-type: none"> <li>• Flip chart, marker pens</li> <li>• Projector and screen</li> </ul>

#### **Session details:**

1) Introduce the concept of data sharing processes. (20 minutes)

Ask the participants to list the types of information they share internally and the information that is shared outside the organization. The discussion might flow into the following matrix:

INTERNAL			EXTERNAL
Who	What data	With whom	With whom
Peer educator	Individual KP registration data	M&E officer	
	Day-to-day service delivery data	Field supervisor/district coordinator	
	Clinic escort data	Field supervisor/district coordinator	
Field supervisor/ district coordinator	Day-to-day service delivery data	M&E officer	
	Escort data from the clinic shared by each peer educator	M&E officer	
M&E officer/ program manager	Consolidated information on contacts, clinic escorts, and condom and lube distribution		Donor

To protect service users' data, implementer safety, and programmatic integrity, the LINKAGES Global Strategic Information Team has developed a checklist (Data Safety Checklist) of actions that should be taken by implementing partners (IPs) collecting, managing, analyzing, and storing such data. IPs and strategic information (SI) backstops should use the checklist and provide detailed guidance on implementation to ensure that adequate protective measures are in place. The checklist is provided in **Handout D**.

Ask the participants to use the Data Safety Checklist (Handout D) to assess the current practices continuously, preferably at the start of any project and every six months thereafter. This can be the self-reported checklist for the M&E and program teams to assess the potential risks and existing practices. It will help them identify the steps that need to be taken to improve the data safety standards outlined in the policy.

In the table below, the left column includes the checklist items from the Data Safety Checklist along with additional information on how to operationalize these items. The right column includes examples of documents (or elements of such documents) that will support operationalization. It also includes illustrative examples in italics to help populate these documents. The illustrative examples are meant only to help IPs think about the content of the documents and are not prescriptive.

Instructions	Actions to be taken
<p>1. Establish protocol/guidelines for sharing data with other partners</p> <p>The protocol should provide guidance on two types of data sharing that often occurs.</p> <ul style="list-style-type: none"> <li>• <b>Type 1: Sharing for analysis and reporting</b> <ul style="list-style-type: none"> <li>○ When sharing information with individuals who are outside the project and/or who will not be providing services, identify the information/data that should not be shared. This includes the service user's name, address, and telephone number.</li> <li>○ Information that is disaggregated should not be disaggregated to the point where it becomes</li> </ul> </li> </ul>	<p><b>Guidance for Type 1 data sharing</b> (illustrative):</p> <p><i>When sharing information for data analysis and reporting, no identifying information (e.g., service user's name, e-mail, address, phone number, date of birth) can be included. Information will not be disaggregated to such a level that it becomes possible to identify an individual. Information on location of individuals, including hotspots, should never be shared</i></p>

<p>identifiable. Location of KP members as a group should also not be shared. Hotspot maps, even without street names, should not be shared. More guidance specific to hotspot mapping and size estimation data collection and handling can be found in <a href="#">Mapping and Size Estimates of Sex Workers: PROCEED WITH EXTREME CAUTION</a></p> <ul style="list-style-type: none"> <li>○ The process for requesting data and the format in which it can be shared (printed, electronic, as a summary report, etc.) should also be described.</li> <li>○ If there are concerns that the ministry or some local official will request identifiable data, it is advised that high-level approval from the National AIDS Council or equivalent authorities be obtained.</li> <li>● <b>Type 2: Sharing data to support service delivery in a way that benefits the individual service user</b> (e.g., when someone is referred between facilities) <ul style="list-style-type: none"> <li>○ The protocol should mention that identifying information can be <b>shared only after the informed consent of the individual KP</b>. The mechanisms in place to share information, such as accompanied referral or written referral slips, should also be described.</li> <li>○ The protocol should also describe the ways in which job responsibilities and geographic areas of work will dictate the identifiable information that is shared with individual IP staff or volunteers. For example, peer educators will need to have information that corresponds to the type of services they provide within their communities. However, they should not have information about individuals in communities beyond their geographic purview and should not have access to clinical results (such as HIV or STI testing results) or other information that a service user shared with a healthcare worker or other program staff (such as experience of violence), unless the service user has consented that this information can be shared.</li> </ul> </li> </ul>	<p><i>beyond the project. Data can be shared upon requests made to ('staff person name and title') as a printed summary and/or electronic reports.</i></p> <p><b>Guidance for Type 2 data sharing</b> (illustrative):</p> <p><i>Identifying information shared with service providers for the benefit of the service user (e.g., HIV status) requires the informed consent of the service user. This means the service user understands what will be shared, with whom, and when. Information should be shared through a referral process that includes clear instructions on the need for maintaining confidentiality.</i></p> <p><i>Peer educators will have access only to identifiable information that they collect or that corresponds to relevant service history (such as condom distribution) in the geographic areas where they work. They should not have specific individual's clinical results (e.g., HIV and STI testing results) or anything else disclosed to other project staff in confidence (e.g., experience of violence) unless they have given informed consent for this to be shared. Peer educators may have aggregate data on incidence of violence in a hotspot in their geographic area to understand HIV vulnerability.</i></p>
---	--

2) Introduce the concept of data destruction processes. (10 minutes)

Tell the participants that you will discuss using the example of the recent closure of GFATM project in your organization. The staff were asked to complete all the records and update all the records/reports in registers, escort slips, and also online in the monitoring and evaluation information management system (MEIMS).

Highlight that usually every data or record has a lifecycle. For example, when the project gets over, the participant’s organization has to hand over all the records and data to the donor. Similarly, there are different terms for each project. The table below carries some recommendations for data destruction processes.

Instructions	Documents to support operationalization (with illustrative examples)
<p>1. List of individual(s) with the right to destroy data (e.g., in case of an impending police raid)</p> <ul style="list-style-type: none"> <li>• Provide the names and positions of those who can destroy identifying data outside of compliance with donor specifications; a general rule of thumb is to keep paper-based records for five years; for organizations with clinical files, follow the Ministry of Health’s rules and policies regarding data storage.</li> </ul> <p>The document should also clearly outline how such a decision can be made and by whom and be reviewed and approved by the donor.</p>	<p>Names and positions of staff members with the right to destroy data</p> <p><i>Destruction of data should be the last option and used only if there are no other alternatives to protect data. Data can be destroyed if it is not possible to protect identifiable data (e.g., police raid is impending or has occurred elsewhere). The decision that such a threat is imminent can be made by (the person’s ‘name’, ‘title’).</i></p>
<p>2. Have a protocol for safe destruction of data/records.</p> <ul style="list-style-type: none"> <li>• Each donor will have its own guidelines regarding how long paper and electronic records must be kept. Follow these guidelines unless there is an emergency that requires earlier destruction of data</li> <li>• Electronic data should be destroyed completely. Note that simply deleting a file does not destroy it. Choose from the destruction options described in <a href="#">Best Practices for Data Destruction</a>.</li> <li>• If needed, paper records should be destroyed using cross-cut shredders, pulverizes, or incinerators.</li> <li>• Destroy CDs, DVDs, and any magneto-optical disks by pulverizing, cross-cut shredding, or burning.</li> <li>• The process of how the data will be destroyed, including in what timeline, should also be stated in the protocol.</li> <li>• Each time data is destroyed, the process for destruction should be described in detail and signed by the person who destroyed the data.</li> <li>• Review the protocol quarterly to ensure that it meets organizational needs and reflects the current staffing structure.</li> </ul>	<p>Guidelines detailing how long paper-based data should be stored and how long electronic data should be stored</p> <p>Specific guidance from the Ministry of Health on the storage of clinical records</p> <p>Guidelines detailing how paper-based records should be destroyed and how electronic records should be destroyed</p> <p>Documentation on past data destruction, including date and method used</p>

Summarize the discussion by highlighting that data sharing also implies safeguarding against its misuse and use beyond the intended purpose. Hence, it is very important that before sharing the data with any external person, even the donor’s representatives, the following should be checked:

- Ascertain the purpose for which data is being requested and shared. Check whether the purpose/instance for which data is being shared falls within the available policy of the donor or the implementing partner.
- Data should be shared only by the person authorized to share the data with the intended user.
- Check if personal data is being asked for and for what use.

End the discussion by highlighting the key takeaways mentioned below.

Key takeaways:

- Data sharing, both within the internal team and with external parties, including the donor, needs to be regulated by the organizational policy.
- Data needs to be safely and securely shared without compromising the identity and other personal details of the service users/beneficiaries.
- Data sharing is the responsibility only of the person who is authorized to do so.
- Data destruction or archiving is a process to ensure that the purpose for which the data was collected is achieved as per the needs of the project and the data does not get misused.

## Session VII: Summing up

Duration: 30 minutes

Objectives:

- To facilitate the participants in recapping the day’s learning and reflecting on their day-to-day work

Show participants the slide below; it summarizes the lifecycle of data in projects.

**Figure 5: Life Cycle of Data** (Source: *Using the Data Lifecycle to manage the data responsibly, OXFAM*)



## References

Bickley, S. (2017). *Security Risk Management: a basic guide for smaller NGOs*. European Interagency Security Forum (EISF). Available at: <https://reliefweb.int/sites/reliefweb.int/files/resources/2157-EISF-June-2017-Security-Risk-Management-a-basic-guide-for-smaller-NGOs.pdf>

East and Horn of Africa Human Rights Defenders Project. (2017). *Stand Up! Security Guide for Human Rights Defenders in Africa*. Available at: <https://www.defenddefenders.org/wp-content/uploads/2017/04/StandUp.pdf>

LINKAGES. (2016). *Monitoring Guide and Toolkit for Key Population HIV Prevention, Care, and Treatment Programs*. Available at: <https://www.fhi360.org/sites/default/files/media/documents/resource-linkages-monitoring-tools.pdf>

LINKAGES. (2018). *Safety and Security Toolkit: Strengthening the Implementation of HIV Programs for and with Key Populations*. Available at: <https://www.fhi360.org/sites/default/files/media/documents/resource-linkages-safety-security-toolkit.pdf>

OXFAM. (2017). *Using the data lifecycle to manage data responsibly*. Available at: <https://oxfamilibrary.openrepository.com/bitstream/handle/10546/620235/ml-rdm-data-leaflet-290317-en.pdf?sequence=6>