CTIP M&E Toolkit: Summary of Data Privacy and Security (Jessie Brunner, 'Getting to Good Human Trafficking Data' and USAID 'Monitoring Toolkit, Data Security Guidance: Protecting Beneficiaries')

This resource provides a basic introduction and guidance into Data Privacy and Security in MEL. The aim is to help the user to understand and think throughout the data management process of a MEL project. It covers some basic guidance on the following:

- Why is Data Privacy and Security relevant to MEL?
- Data Management Plan: what is it and what to include.
- Data Security: what it is and some recommendations.
- Protecting Beneficiaries: how to protect beneficiaries, especially Personally Identifiable Information.
- Data Storage: what it is and options to store your data.
- Data Sharing: some recommendations to consider when sharing data.

I. Data Privacy and Security in MEL

Why is Data Privacy and Security relevant to MEL?

Data owners have a responsibility to hold, use and manage data pertaining to others in a safe and responsible manner, in adherence to the applicable laws and regulations. Inappropriate access, use or loss of data can have significant negative consequences for users and organizations. Data are collected and used in various ways in MEL activities so the considerations that apply to Data Privacy and Security are fundamental to undertaking good MEL in a responsible way, safeguarding the individuals and organizations involved – including your own.

II. Data Management Plan

What is a Data Management Plan?

A data management plan defines an entity's approach to data security to ensure proper data maintenance and provide backup plans to address potential challenges. It lays out a strategy for the entirety of the data lifecycle: system design, collection and storage of data, analysis, and data sharing. Comprehensive data management systems need to consider:

- What kind of data does your organization/entity collect?
- What data do you create?
- How do you store your data?
- How do you ensure secure, appropriate access to your data?
- When and how do you delete/dispose of your data?

When developing a plan, you must be aware that each component could potentially impact the privacy and security of the data subject. The Plan may need to be revised to accommodate sectoral learning and developments.

What should you include in your Data Management Plan?

The following is a list of potential components of a data management plan (it might vary according to your entity's needs).

1. Consent Procedures: ensure that clear policies on informed and active consent are in place and both known and practiced by staff. Participants need to understand the processes, the possible consequences, and how their personal data is going to be used.

2. Data inventory: consider the data you already have, evaluate what you collect and how you use it to meet your objectives. This helps to ensure that:

- A policy of data minimization is followed: limiting the personal data you collect and setting appropriate, timely disposal procedures.
- Potential of data breaches (the release of confidential data into an untrusted or insecure environment) are limited.

3. Data archiving: the process of appropriately preserving data that allows for easy reference and use.

4. Data disposal: the process by which data is destroyed securely and responsibly. You need to establish the amount of time you will keep your data; some data privacy laws stipulate a period of time at which data must be destroyed.

5. Data security: keeping data secure → see next Section, *III Data Security*.

6. Inventory of hardware and software and how they are used within your organization.

7. Establish brief but descriptive naming conventions: following a standard procedure for naming documents ensures consistency and makes retrieval easier (i.e., using underscores "_" instead of spaces in the file name can help ensure compatibility across different computer systems). Also, if working on a document over time, you may want to consider version history in the name "v1" or "vFinal".

8. Lists of people accessing the data: individuals working with and accessing the organizational data (including their roles, responsibilities, and permission levels).

9. New Staff Training: outline how new staff will be trained on data systems and how organizational data on personal devices will be secured when staff leave.

10. Internal and External data sharing and disclosure processes: how is the sharing of data managed? → see Section *VI. Data Sharing.*

11. In-person data collection: for in-person data collection, consider if data entry will be done in the presence of respondents or if will it be input later, and consider how data entry will affect the nature of the interaction.

12. Case management: for those working on case management, establish how often data will be updated for a given individual and how progress will be tracked.

13. Policies/regulations: Document the governing policies/regulations related to data in the places where you work (or where digital data pass-through)

14. Ensure data quality: a policy for ensuring data quality, including data cleaning.

15. Backup plan: the means by which you ensure that you have a copy stored in a different location to your primary storage but with the same security and privacy measures in place (if your digital data are stored locally, as opposed to on the cloud where the backup is typically automatic). Remember that a backup is essentially a snapshot of a file at a given point in time and does not automatically update with the original file.

16. Data cleaning and checking for accuracy: consider creating a mock data set for data entry and cleaning for your team to practice.

III. Data Security

What is Data Security?

Data security prioritizes keeping information secure. Due to the often-sensitive nature of the data collected in the anti-trafficking field, data collection presents risks to the data subject and their families and personal networks. Therefore, data security is key to ensuring subjects' safety and protection. It is impossible to guarantee security completely, but a certain level of protection has to be achieved to start collecting data in the first place: "We should not be collecting digital data until we have a secure, reliable way to store that information" (Brunner, p.62).

In order to secure your data, you must ensure the following:

- Prevent unauthorized access to the data.
- Prevent unauthorized use of personally identifiable information → see Section *IV Personally Identifiable Information*.
- Ensure that partners have appropriate safeguards in place to secure the data collected.
- Restrict access to offices and workspaces via the use of key fobs or similar mechanisms.
- Prevent unauthorized computer access through password protection.

When is data insecure?

Data may be insecure in transit or 'at rest', and in either physical or electronic formats. When insecure, data can be accidentally altered or accessed by malicious third parties.

- Data in transit: emails or files attached to email → data can be intercepted, downloaded, and read by third parties without either the sender or receiver's knowledge unless properly encrypted or password protected.
- Data 'at rest' refers to the storage of data in physical or virtual storage systems.
- Data stored electronically on an organization's network can be insecure on-site or remotely if appropriate security measures are not put in place.
- Hard copies of documents, if not securely stored, may also be vulnerable.

What are some common challenges related to data security?

Some common challenges may be:

- Lack of awareness of how data is stored and backed up (i.e., in-house servers vs. cloud-based storage)
- Sharing account log-in information between multiple users
- Lack of awareness of encryption to secure data or lack of access to appropriate software to enable its use.
- Wi-Fi network and password information on display in public places.
- Website being hacked and pages remaining down over time.

How can you improve your data security?

There are some steps you can incorporate into your organization's practices:

- Assess your current practices, giving particular attention to any vulnerabilities or potential threats, and develop a plan to mitigate or address these concerns.
- Establish and revise protocols to mitigate new risks. In particular, at key moments, such as when new features are added to your data systems or when organizational policies or programs change.
- Ensure that all staff understand the risks and their responsibilities in being a data custodian; the responsibility for protection is shared among all personnel in a given organization.
- Ensure that all staff are familiar with relevant organizational policies, procedures, and updates.
- Within an organization, even if sharing device, it is recommended for everyone to have unique log-in credentials and passwords to track data access (many digital data systems catalogues who is logging in when and from where, and which files are accessing).

Legal environment:

- Consult both national and regional legal frameworks when designing data protection policies, especially for highly sensitive personal data. You must consider the laws not only of the localities in which your entity is registered, but also there you operate, where your data is stored (and pass through) and where your clients/subjects reside.
- Ensure all staff are familiar with relevant local and national laws governing the protection of data.

Emergency plan for data breaches:

- Have an emergency plan for data breaches. Develop a list of people that goes beyond your organizational expertise. Make a plan for the potential loss of a device that contains sensitive information. In case of a security breach or other violation, you must notify the data subject that has been compromised and consider what protective resources you might provide them.

Secure physical environment:

- The security of the physical spaces (offices and work environments) must be considered when making decisions about data collection. For instance, working in a public setting is less secure, as is connecting to public Wi-Fi networks.

Recommendation: "Conduct an assessment of your organization's current practices around security, giving particular attention to any vulnerabilities or potential threats, and draft a plan for how to address these concerns. This plan should include provisions for how staff will be coached on data security protocols and should be revisited regularly to mitigate potential new risks, particularly at key moments,

such as when new features are added to your data systems or when organizational policies or programs change" (Brunner, p. 62).

And some steps to incorporate into your individual daily practices:

- Select strong passwords (see Brunner, p.66 for some tips)
- Add a layer of log-in security: biometrics (fingerprints, retina scans, voice recognition).
- Secure not only computers, but also smartphones, tablets, data storage devices such as external hard drives and USB devices, digital cameras, and printers or copy machines.
- Set your devices to lock automatically after a short interval and require a password to log in.
- Secure personal devices in the same way you would secure a work computer or device if these contain or access sensitive data.
- Encrypt data: converting readable text into text that cannot be read without a key.
- Never include personal details in the subject line of an email.
- Do not post the network or password information for your Wi-Fi out in the open.
- Set aside one day each year for file clean up, wherein all team members take a quick inventory of all their records and dispose of old paper and digital files that are no longer needed.
- Be aware of phishing and be able to identify phishing emails.

How to delete/dispose of data?

- Paper files: shredding or incineration
- Digital fines: it is not enough to simply delete from your computer, it is important to use wiping tools, not only to delete the information but to also mask its previous location and ensure any digital footprint has been removed. Make sure you also wipe secondary devices such as flash drives or digital cameras.

It is important to bear in mind that applicable personal data privacy laws may affect your right to delete data.

IV. Protecting Beneficiaries: Personally Identifiable Information

What is Personally Identifiable Information?

Personally Identifiable Information (PII) includes any kind of information that can be used to directly or indirectly distinguish or trace an individual's identity: name, physical or email address, Social Security Number or government-issued ID number, biometric records (including fingerprints and voice recordings), contact information, gender, race, geographic location, and full-face photographic images. PII is one of the most risky types of information.

How can you protect Personally Identifiable Information?

Some recommendations include:

- Collect and report only the minimal amount of data necessary for explicit purposes, not only for convenience.
- Anonymize data to gather and/or report information. This can be done by using a unique identifier code/name (randomly generated number or string of characters).

A key matching the unique identifier code/name with the original name information should be encrypted and stored securely, separately from the full data set.

- Store hard and soft copies of PII securely while restricting access to only those staff who need it.
- Appropriately delete, destroy, or otherwise permanently dispose of all paper and electronic copies of PII once their purpose has been served.

V. Data Storage

What is Data Storage?

Data must be safely and securely stored while remaining accessible to those who need it in their work. There are different ways to store your data, this can include hard copies locked in file cabinets, password protected digital files, and sophisticated cloud-based management systems with role-based access controls.

How can you store your data?

Data is usually collected in hard format (paper copy) before being transcribed electronically. The USAID Monitoring Toolkit suggests some ways to secure your data:

Hard copies files:

- Store data records in locked file cabinets in a restricted access workspace. Take care not to leave sensitive documents on desks or in shared workspaces.
- Ensure that all documents are collected from public spaces (e.g., following workshops, training, etc.)
- Shred data records immediately once they are no longer needed, e.g., following transcription or the required storage period expires.

Soft copies files:

- Passwords protect or encrypt documents and the folders they are being stored in.
- Store sensitive information offline, or in locations not connected to the internet.
- Encrypt email.
- Ensure email attachments are password protected. Passwords for attachments should never be shared within the email they are attached to.

Some advantages and disadvantages of different options to store digital data:

	Advantages	**Disadvantages**
Local/Personal computer (or other electronic device)	Clear control of the data at the individual level, secured from outside access if properly encrypted and securely stored	Subject to loss, theft, confiscation, destruction; unable to access from remote locations; no backup

Private network	Data are more resilient to loss of any single device, clarity of control at organizational level, easy to collaborate, frees up hard drive space on devices	Challenges to securing data, cost of maintaining the network, potential reliance on outside support, susceptible to data loss
Cloud-based storage (*)	Generally affordable, potential IT support from provider, data backed up to physical servers in multiple locations, risk of data loss highly reduced, frees up hard drive space, easy to share/collaborate, accessible from multiple locations through log-in	Questions of control over the data may be unclear, data access controlled by a third party whose policies may fluctuate

Table 1 - Source: Getting to Good Human Trafficking Data (p.58-59)

(*) If using cloud-based storage, it is recommended to "look for providers who value data protection and privacy, offer reliable and rapid customer support, and are trusted in the anti-trafficking field or human rights more broadly" and, "you should negotiate an exit strategy should you wish to terminate your account that includes full retention of your data for your organization and complete deletion from their servers" (Brunner, p.59).

VI. Data Sharing

When sharing data, you must have permission from the data subject to disclose their information outside the organization. Additional consent must be obtained if the data is used for a different purpose than the original agreement. For further details, see Brunner p.75.

What do you need to consider?

1. Create a data-sharing plan: create a data-sharing plan addressing the questions below. It is recommended to appoint someone within your organization who oversees and is accountable for these processes.

- What data will be shared and in what form?
- What data documentation will be shared along with the data to help inform its accurate interpretation?
- With whom will your organization share data?
- How will you determine what data are appropriate to share and not?
- How will the data be received and accessed?
- How will sender and receiver ensure data are protected in transit and long term?

2. Draft a data sharing agreement: for information being shared privately between entities, it is recommended you implement a data sharing agreement or non-disclosure agreement (NDA) between your organization and other outside entities. Core elements should include, but are not limited to:

- A clear description of how the recipient will use the data.
- Indication that ownership remains with the organization sharing the data (and the data subjects)

- Recipients must agree to use the data for the purpose outlined therein and not to disclose, release, sell, or otherwise grant access to that data to other parties.
- A clear description of how the recipient will ensure the data remains confidential, including how they will maintain control of the data; if data are accidentally disclosed by the recipient, this should be reported immediately to the sharing entity.
- In the case of de-identified data, the recipient shall not make an effort to re-identify the data subjects.
- Stipulated timelines for data and destruction

3. Protect the identity of data subjects: data de-identification is the process by which you prevent a person's identity from being connected to their data. Some guiding questions to identify whether data are PII and therefore need to be de-identified before sharing:

- Do the data obviously relate to a particular individual?
- Can an individual be identified from the data directly, or from the data when combined with other relatively accessible information?
- Could the data be used to directly impact or affect actions or decisions related to an individual?
- Do the data focus on the individual as the central theme, as opposed to an event or other subject matter?

4. Consider your medium for sharing: different methods for sharing offer unique benefits and potential drawbacks.

- Physically (paper files, digital files on an external hard drive, USB key or another device): you know who is receiving the data, but it opens up opportunities for the records or devices to be lost or stolen.
- Text messaging (ideally through an app with end-to-end encryption): ease but users should be verified, and practitioners should avoid sending sensitive data – WhatsApp and Signal employ the same encryption methods, but Signal does not store metadata on its chats and is open source.
- Regular email: not very secure as it can be easily hacked. Encrypting files can help but it is recommended that encryption keys be shared over a secondary, secured medium → Virtru and FlowCrypt for instance.
- Cloud services (Dropbox, CertainSafe, iCloud, Microsoft OneDrive, and Google Drive): convenient mode and can be made more secure through encryption.