Monitoring Toolkit

DATA SECURITY GUIDANCE: PROTECTING BENEFICIARIES

Introduction

This resource complements ADS 508 – USAID's policy on its privacy program – by providing guidance on protecting monitoring data across the Program Cycle. As a best practice, data security approaches should be detailed in a data management section of the Activity Monitoring, Evaluation, and Learning (MEL) Plan.[1]

Why Do USAID Data Need to be Secure?

Data security is a key practice to ensure good quality data and the protection of USAID's partners and beneficiaries. As stated in ADS 201, Missions and Washington Operating Units must protect USAID beneficiaries by preventing the unauthorized access and use of personally identifiable information (PII) collected for indicator data reporting. This includes ensuring that partners have appropriate safeguards in place to secure data collected for project and activity planning and management, monitoring, evaluation, accountability, and learning purposes.

DATA QUALITY

USAID staff and implementing partners should be operating with at least a basic level of data security as part of their data management system and overall operating procedures. This basic level of data security often includes, at a minimum, restricting access to offices and workspaces via the use of key fobs or similar mechanisms, and preventing unauthorized computer access through password protection. Security measures such as these prevent fraudulent data manipulation or the premature public release of data.

PROTECTING PEOPLE

In the process of implementing activities, the security of USAID's beneficiaries or partner organizations may inadvertently be put in jeopardy through the mishandling of information. The exposure of such information may physically, legally, or financially endanger the people or organizations engaged with USAID. More advanced security measures may be warranted on an activity-by-activity basis, depending on where the activity is being implemented, the type of data being collected, and who the beneficiary groups might be. USAID and its partners must consider whether their partners or beneficiaries are at risk and how to mitigate these risks, including potential cost implications.

How Can Data be More Securely Protected?

Data may be insecure while in motion or at rest, and in either physical or electronic formats. This means that data could be accidentally altered within the activity by implementers, or be intentionally accessed by

[1] ADS 508 details USAID's internal policies and procedures for protecting programmatic data, and specifically personally identifiable information (PII).

potentially malicious third parties, at any point. Data in motion, such as emails or files attached to emails, 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 is accessible either on site or remotely if appropriate security measures are not put in place. Similarly, hard copies of documents, if not securely stored, may be vulnerable.

When deciding the most appropriate way to protect data, it is important to consider what the data are, the origins of the data, and the current state of data files. Data are frequently collected in hard format (meaning paper copy) prior to being transcribed electronically into a soft format, such as word processing documents, spreadsheets, or databases. Here are some methods to securely store or handle various kinds of data:

- **Personally Identifiable Information (PII)** is one of the most commonly at-risk types of information. PII includes any information that can be used to directly or indirectly distinguish or trace an individual's identity, such as their name, address, Social Security Number (SSN), biometric records, contact information, gender, race and geographic location. This information can be used on its own, or combined with other personal or identifying information, for example, date and place of birth or mother's maiden name. Such information is frequently gathered through USAID activities, often in the form of attendance lists from trainings or workshops, rosters of participating individuals or organizations in specific interventions, or even contact information for local sub-contractors or partners under USAID awards. While a risk that should be mitigated across all USAID activities, the theft or inadvertent loss of PII may be of particular concern for activities working with vulnerable populations where physical safety may be in jeopardy. For official USAID requirements for handling PII please see ADS 508.3.9. More generally, some ways to protect PII include:
    - Collecting and reporting only the minimal amount of data necessary for an explicit purpose; PII is not something to be collected for convenience purposes.
    - Anonymizing data can be an effective way to gather and/or report information while protecting beneficiaries.
    - Storing PII securely, both in hard and soft copies, while restricting access to only those staff who need it.
    - Appropriately deleting, destroying, or otherwise permanently disposing of all paper and electronic copies of PII once their purpose has been served.

- **Information on Programming or Strategy Implementation**, in some cases, may also need to be protected to ensure effective and uninterrupted execution, while at the same time balancing the mandate to share programmatic data and information transparently where appropriate. In some contexts, if implementation information becomes compromised it has the potential to disrupt programming in one of two ways: (1) if beneficiaries become aware of the intervention approach before it is appropriate, for example when piloting an innovative new approach, then it may alter their behaviors and have unintentional effects on the activity's ability to achieve its objectives, and (2) if information on how and when an activity will be implemented is accessed by groups or individuals who do not support that activity, they may attempt to thwart the implementation of the activity, possibly using violence. Implementation information can be protected by:

  - Only sharing planning information with partners on a need to know basis.
  - Carefully vetting potential beneficiaries in sensitive areas to ensure their interest in participating.
  - Establishing a clear set of protocols for how and when information will be shared publicly.

- **Hard Copies of Information** may have contractual requirements associated with them in regard to how long they must be maintained or how they must be destroyed. Securing data in hard copy formats may be done through:
  - Shredding documents immediately following transcription, use, or required storage period.
  - Storing documents in locked file cabinets in a restricted access workspace.
  - Ensuring all documents are collected from public spaces (e.g., following workshops, trainings, etc.) with none being left for disposal by contracted facilities such as hotels.

- **Soft Copies of Information** are generally best protected through ever evolving cybersecurity practices and ensuring all staff and partners have a basic working knowledge of cybersecurity best practices.[2] Beyond implementing cybersecurity protocols, securing soft copies of information can be done through:
  - Password protecting or encrypting individual documents and folders they are being stored in (USAID approved encryption tools are Winzip and Adobe).
  - Storing sensitive information offline, or in locations not connected to the internet.
  - Encrypting email.
  - Ensuring attachments to emails are password protected (passwords for attachments should never be shared within the email they are attached to).

USAID takes the security of its partners and beneficiaries very seriously. Securely storing data, including performance data of USAID's activities and work, is paramount to effective development practice.

[2] US CERT has good free resources on these practices: https://www.us-cert.gov/security-publications