(See: Responsible Data for M&E in the African Context)

TIP SHEET 9

How to develop a data retention policy

A data retention policy could include the following content:

- What is the purpose of the policy?
- Who must follow the policy?
- Who is responsible/accountable for administering the policy and ensuring compliance?
- A note that you might, for certain legal reasons, be forced to keep data longer.
- A list of the types of data included in the policy.
- The period for which each type of data will be retained (see more information on this below).
- Any specific orientation on how the data will be treated while retained (e.g. password-protected, only accessible by role, etc.).
- Any specific orientation on how data will be anonymised or aggregated.
- Any specific orientation on how data will be destroyed.

Based on the policy formulated, it is advisable that data in the system is flagged by category, so that you receive automatic notifications indicating when it is necessary to aggregate or delete data. Data can then be reviewed periodically based on the automated notifications (not auto deleted) and data that is no longer needed can be deleted or aggregated.

In addition to the data retention plan, processes should be put in place to ensure that the plan is followed and someone should be assigned the responsibility of stewarding the data along its lifecycle – follow the link for a sample data retention policy.

Align your data retention policy with your informed consent process and other privacy-related policies

As can be seen from the description above, data retention plans are the basis of consent processes, terms and conditions, privacy policies, or any other information provided to data subjects about the use of their data. The plans should also guide how data is handled and stored and should provide details on who is authorised to access the data and any systems that manage the data.

▶ **See Stage 2** for more orientation on consent

At the start of any new partnership or initiative involving data, it is important to establish and document appropriate data retention periods and these should be based on the following:

- Data source (from whom/where is the data collected).
- Type of data.
- Reason for keeping data.
- Personal data or sensitive data.
- Will data be aggregated or de-identified or anonymised and when will this happen? (if it is not subject to a retention period).
- Where and how will the data be stored?
- How long will the data be held?
- How will data be destroyed?

Ensure that you have a data management plan for the termination of your programme or M&E initiative.

The absence of a plan on how to terminate a data collection exercise risks that the data can be left unsecured or improperly disposed of, creating an opening for a data breach or other type of data misuse. Therefore, it is important to have a plan from the start on how a project will terminate, whether it will be sustained, and what will happen to any data collected as part of the project or M&E effort. If you do not plan to delete data at the conclusion of the project, you will need to decide on and allocate a budget for maintaining the data and keeping it secure.

▶ **See Guidelines** for designing and planning for M&E in Stage 1