USAID AMPATH Uzima

Telephone: (+254)532033471/2 | Postal Address: P.O. Box 4606-30100, Eldoret, Kenya | Email: info@usaidampathuzima.or.ke

OVC - Job Aid on Data Protection Protocols

Confidentiality, Documentation, Record Filing and Information Sharing

Data protection relates to the protection of all personal data collected, either through individual discussions as well as the receipt of secondary data. Agencies involved in case management must develop data protection protocols based on the principles of confidentiality and "need to know", with the ultimate aim of safeguarding the best interests of the child. Data protection protocols serve as a guide for what information to collect; how the information will be used; and how the information will be stored. All staff involved in the case management process should be aware of the data protection protocols.[1]

Confidentiality

Data protection protocols are based on the principle of confidentiality. Confidentiality is the preservation of privileged information. The information learned from work with a family and children is necessary to provide services to the child or family and is shared within the development of a helping, trusting relationship. All information concerning children, caregivers or family members is confidential. This means that Case Workers are not permitted to disclose child, caregiver or family names, locations or to talk about them in ways that will make their identity known for any other purpose than the provision of services and on a need to know basis.

Confidentiality and client consent: The Site Improvement Monitoring System (SIMS) for case management recommends that Case Workers should adhere to applicable local, state, and federal laws, as well as employer policies governing the client, client privacy, and confidentiality rights, and act in a manner consistent with the client's best interests. Case Workers should sign confidentiality agreements that detail these policies. At a minimum, policies should outline how Case Workers should instruct Case Workers to keep case files and any documents identifying clients in a safe space and not discuss the details of a case with anyone not directly involved in the case or who hasn't signed a confidentiality agreement. Case Workers should seek to obtain the child's and caregiver's written acknowledgement that he or she has received notice of privacy rights and practices, and consents to services. Case Workers should also ensure that the child and caregiver are aware of the costs and benefits of participation in the OVC program, including potential risks to participation or alternatives to participation in the OVC program, and that they have the right to refuse or terminate services at any point, as well as the potential risks and consequences related to such a refusal.

Confidentiality protocols should be based on the understanding that the child/family owns the case information and that only with the **family's consent** (child's assent) the information can be shared beyond the case management relationship, unless ordered by an authorized statutory entity such as a court.

During enrolment, the Case Worker should ensure family consent s is received and documented. The implications of sharing this information should be fully explained.

Documentation & Record Keeping

All case management work will be documented following established information management and data protection Protocols centered on the **family and child's case file** and described within this document. Documentation includes both written paper records and electronic case management records.

1) **Case files**

Individual family case files should be created for each case, based on the individual family and include documents for each child within the family with key information presented in a standard, structured way. It should include the standard forms and case notes that document each step of the case management process.

As a case progresses, forms and notes should be accurately and thoroughly filled out and stored in the file.

These files should be kept in a **secure location** with restricted access such as a **locked cabinet**, or **password protected** if electronic case files are used.

There should be clear and coordinated data collection, storage and analysis protocols in place.

The retrieval and any other movement of files from the filing cabinet must be documented within a register to ensure that case files can be tracked between Case Workers, supervisors, M&E and program staff. The staff retrieving the file should complete a register. Below is an example that can be used.

Client name	Unique Identifier	Name of Case Worker requesting the file	Date of retrieving the file	Date of return of the file

When a file is retrieved, it is common practice to place a holder to indicate that it has been retrieved. This can be an empty folder or a card with the name and number of the file that has been retrieved, as well as the name of the person who has removed it.

2) **Unique Identifier**

The case should be assigned a **unique identifier** for confidentiality purpose and effective tracking of individual cases**.** The unique identifier should be a code based upon an agreed upon standard format and **should not identify the family or child**. The format may indicate areas of identification or areas of origin but should guarantee anonymity of the family and the child.

The code should be used to refer to the child's case either verbally, on paper or electronically (including in word documents, emails, skype conversations, etc.) in place of any identifiable information such as name or date of birth.

All files should be stored according to the allocated code.

The unique identifier should be marked on the front of the case file. The name of the

The Site Improvement Monitoring System (SIMS) for case management notes that Case Files can be paper or electronic, but regardless should be easily accessible by the case manager. They should be stored in a safe and confidential manner (typically in a locked file cabinet and/or password-protected electronic file or encrypted mobile device). Files should include documentation completed prior to referral to the OVC program, completed screening or prioritization forms, enrollment forms with basic bio data information, a completed initial assessment and any reassessments and assessment reports, initial case plans and any updated case plans, case notes from monitoring visits, documentation associated with referrals or documentation of completed actions (e.g., referral return slips, school progress reports), and documentation of the circumstances of case closure.

family should not be recorded on the front of case files. Below is a sample unique identifier system if no government or organizational system exists.

3) **Database**

Selected information should be entered into the database in a secure and confidential manner. The electronic data should be **password protected** and the password **changed on a regular basis.** Information should be transferred by **encrypted or password protected files** whether this is by internet or memory sticks. Memory sticks (USBs) should be passed by hand between people responsible for the information and be password protected, and the file erased immediately after transfer. Ensure that the file is also permanently erased from the recycle bin file of your computer.

A regular backup system should be in place. Typically, an on-site back up is done on an external hard drive which is kept locked in a filing cabinet. Ideally, a second off-site back-up in a second location (for example head office) should be setup for secure storage in a pre-defined centralized location. The reason for having an off-site back-up is so that the data can be retrieved if the main database becomes damaged. The offsite back up is often done through electronic sharing of the database to the designated receiver as an encrypted, password-protected zip file.

Computers should be fitted with **up-to-date anti-virus software** so as to avoid corruption and loss of information.

Staff responsible for data entry and management should **be included in all case management related training and capacity-building activities** to ensure they understand the processes, and especially data protection/confidentiality issues.

Information Sharing Protocols

As multiple agencies or government departments are working together to address the needs of families and children, through the provision of multiple services and referral pathways, it is essential to also develop **agreed information sharing protocols**, which define what information about the family and children should be shared, when and with whom. How this information will be shared, verbally, electronically or through a paper system, also needs to be defined with appropriate procedures to ensure that the confidentiality of the family and child is protected and respected at all times. [2]

Confidentiality agreements need to be signed when confidential information is being shared among multidisciplinary actors participating in an integrated case management effort such as case conference. An example of a **confidentiality agreement** for case conference meetings can be found at the end of this job aid.

Confidentiality Policy

Confidentiality is the preservation of privileged information. The information learned from work with a family and children is necessary to provide services to the child or family and is shared within the development of a helping, trusting relationship. All information concerning children, caregivers or family members is confidential. This means that you are free to talk about the OVC project, and about the program and your position, but you are not permitted to disclose child, caregiver or family names, locations or to talk about them in ways that will make their identity known.

No information may be released, even to other organizations or agencies, without appropriate authorization and documented consent from children and caregivers. This is a basic component of social work ethics.

As someone providing case management to families, you are expected to respect the privacy of children, caregivers and families and to maintain their personal and household information as confidential. All records dealing with specific children and families must be treated as confidential. General information, policy statements or statistical material that is not identified with any individual or family is not classified as confidential. Staff members are responsible for maintaining the confidentiality of information relating to other staff members and volunteers as well.

Failure to maintain confidentiality may result in termination of employment, or other corrective action.

Certification

I have read the policy on confidentiality. I agree to abide by the requirements of the policy and inform my supervisor immediately if I believe any violation (unintentional or otherwise) of the policy has occurred. I understand that violation of this policy will lead to disciplinary action.

.

Name _____ Signature _____ Date _____