DATA MANAGEMENT AND PROTECTION STARTER KIT

TIP SHEET 4 REGISTRATION

elan
The Electronic Cash Transfer Learning Action Network

WHAT IS REGISTRATION?

Registration is the process of collecting information on program participants so that your team has a clear record of who is participating and a means to verify participants' identity throughout the program lifecycle. Registration is also one of the first opportunities to demonstrate responsible data management.

While all humanitarian programs collect substantial personal information about participants (and sometimes potential participants and/or alternates), e-transfer programs often require that personally identifiable information (PII) is provided to financial service providers (FSPs) as well. The type of data collected may include participants' contact details (addresses, telephone numbers, etc.); information about family members; and/or sensitive information, such as details about a participant's disability or political affiliation.

WHAT HUMANITARIANS NEED TO KNOW:

Registering e-transfer program participants well requires balancing multiple needs: needs for compliance, efficiency, accuracy and the privacy of individuals' sensitive information.

- Conduct a Privacy Impact Assessment (PIA) prior to registration to understand the threats and risks associated with collecting personal data *(see PIA Tip Sheet for more information)* in your operating context.
- Review your data needs, ensuring that you collect only the minimum amount of required data *(see Data Minimization Tip Sheet for more information)*.
- Understand what Know Your Customer (KYC) regulations apply to FSPs in your country of operation and negotiate so that they collect the minimum amount of required data *(see KYC Tip Sheet for more information)*.

Informed consent vs. informing of risks/data rights

You have a duty to inform program participants about the planned use and sharing of their data, as well as the measures taken to secure it. After this introduction, program participants should be able to choose whether to give their informed consent for the use of their data. Use this opportunity to share with participants how they can update any data associated with their program registration (e.g. new family members, change of address). Annex A of the Cash Learning Partnership's (CaLP's) *Protecting Beneficiary Privacy: Principles and operational standards for the secure use of personal data in cash and e-transfer programmes* includes a sample informed consent form.

In cases where declining to provide personal information would mean not receiving emergency assistance, participants cannot provide informed consent. In these situations, which are common in emergencies and e-transfer programs, humanitarians should explain the purpose of collecting certain information, with whom it will be shared, and the measures taken to keep this data safe. Take time also to explain any potential risks associated with collecting this data, as well as participants' data rights, which vary based on your country of operation.

ID types

A range of documents and/or processes can be used to verify a program participant's identity. In general, a reliable ID form has a unique identifier code (e.g., number), is difficult to tamper with or duplicate, and is issued through a trusted process. In some cases, it may also include biometric information (such as a picture or fingerprint). Since you will rarely be able to rely upon a single ID type, select a preferred form of ID for your program, with a list of possible alternatives or combinations when the preferred ID is unavailable. Below we list some common ID types and the advantages and disadvantages of their use.

Common ID Types and their advantages and disadvantages

IDENTIFIER/ID CARD TYPE	ADVANTAGES	DISADVANTAGES
National government-issued ID card **Note that other government-issued IDs (e.g., driver's license, birth certificate) may be used in some cases*	• Most commonly accepted form of ID by FSPs • Uses existing local ID systems (rather than creating a parallel system) • Often includes a clear unique identifier code (although this is not the case in every national system)	• May not be available, particularly after acute emergencies • In some areas, vulnerable populations are less likely to have national ID cards • Does not always contain verifiable biometric information
ID card issued by another organization	• Can be faster than issuing your own program IDs • Avoids cost and energy to create duplicate ID cards • May have coverage that aligns with your participation criteria (geographic, vulnerability)	• Unlikely to meet KYC requirements for opening an account • Unlikely all program participants possess this alternate ID card • May doubt the quality of authentication and verification performed by organization issuing the ID card
A unique program ID card created by your organization *(e.g., smart card, participant card)*	• Can be used for multiple distributions if no other ID is available • Can be issued to populations lacking national or other program ID • *Consider this: If your program participants are to be linked to other programs, try to have the programs use the same unique identifiers*	• Unlikely to meet KYC requirements for opening an account • Costs associated with card design and printing • *Consider this: Although this can increase the amount of time and money it takes to print cards, it is advisable to print the ID cards outside the intervention area to reduce the risk of fraudulent card production.*
Verification by community leaders	• Enables rapid distribution in conflict/natural disaster settings (avoids card printing and distribution time and enables rapid group identification) • Allows populations without formal IDs to participate • Better for blanket/one-off distributions than multiple/targeted distributions	• Does not meet KYC requirements • Difficult to use in repeat/ongoing interventions • Relies on the integrity of community leaders and cross-checks • Slower verification process • Does not provide a unique identifier

Creating a program information system that works

Registration also requires the creation of a program's information management system. How you collect and organize registration data will affect how easy it is to conduct program monitoring and troubleshoot issues reported by participants.

Before beginning the registration process, establish clear protocols for how information will be collected and structured (e.g., What data fields will participants be required to fill out? What will they look like? How are dates and age entered?) This way, compiling individual registration event data will create a full and uniform participant database. If you are jointly conducting registration with an FSP, make sure your systems for data capture are compatible.

Unique identifier (ID) codes

In e-transfer programs in particular, it is critical to maintain a unique ID code for each participant. Unique ID codes facilitate clear, usable databases, since searching by number is much easier than searching by name.

ID codes should be globally unique; in other words, they should not be repeat in any other ID card. A globally unique ID code can include a prefix with the agency and program name (e.g., mc-ecap-0001), using software to generate a unique ID code. Some sophisticated registration systems can also generate two ID codes: a longer, unique ID code used within the information management system (or encoded on a smart card) and a corresponding user-friendly ID code printed on the card. (An example of this is the last four digits of a credit card – usable to distinguish cards locally, but linked to a longer number to distinguish from cards in a larger system.)

When collecting and recording unique ID numbers, set up a process whereby the ID code is entered twice if manually entered; scanned with a barcode scanner; or used in a formula that can identify mismatches.

WHAT HUMANITARIANS CAN DO:

Different concerns apply when you are conducting registration yourself, when your FSP is registering program participants or when you are receiving registration lists from another source (e.g., a local partner).

When your organization conducts registration directly

Segregation of duties is an important, but often overlooked, component of safeguarding data during registration. Programs tight on staff will often combine the process of collecting, processing and verifying registration data into one team. To minimize data manipulation and fraud, however, it is important to segregate these tasks.

The steps involved in registration include:

- Train personnel involved in registration process, define team composition and division of tasks, consider potential challenges between the information collectors and respondents (such as language barriers and gender norms).
    - » Define roles and tasks (data collection, data cleaning, data processing and backing-up) in standard operating procedures (SOPs).
    - » Train teams on all elements of the participant registration process: data protection principles, informed consent and workflows. Explain the registration objectives and highlight any data security risks and mitigation strategies identified during your PIA. Introduce SOPs and applicable protocols. *(See PIA and Sharing Tip Sheets for more information.)*
- Conduct a post-training skills check and address any knowledge gaps.
- Monitor the registration process and provide mentoring and feedback. At the beginning of the registration process, teams should regularly check the quality of data collected (i.e., blank fields, differing usage) to identify any gaps.

When your organization conducts joint registration with your FSP

- Define what information your FSP requires, who will collect the information and how information will be shared between your organizations.
- Plan a back-up process with your FSP for situations where a program participant lacks minimum documentation to open their e-transfer account; note this alternative process in your standard operating procedures (SOPs).
- When conducting joint registration events, consider having your FSP collect program participant information required for opening an account at one station, while your organization collects any additional data at another station. At the end of each event, combine relevant records. This ensures that both you and your FSP have collected information critical to each of your processes in your preferred way and can speed the registration process for program participants

When your agency is receiving registration lists from another source

In emergencies, humanitarian organizations will often receive program participant lists or referrals from other groups (e.g., local partners, colleague agencies, UN bodies or government lists). If you receive participant lists in this way:

- Check whether participants gave consent to share their data when the original list was created. (This is more likely to be the case if another NGO created the list and much less likely if it came from a local government body.) If consent was not gathered, determine how to communicate with data owners before using their information by utilizing any contact information available.
- Cross-check participant eligibility criteria and verify a portion of the list. The spelling of participant names and location can also pose a challenge. Ask about collection procedures so you know how best to use the data and can track the data provenance *(See RAD Tip Sheet for more information)*; use or assign unique identifiers where possible.
- When receiving referrals from other agencies, do your best to obtain all the data points you need to implement your program (e.g., telephone numbers if you plan to conduct post-distribution monitoring by phone). You might consider collecting additional data at other, regularly-scheduled events such as trainings, disbursements or post-distribution monitoring.

ADDITIONAL RESOURCES:

Cash in Emergencies Toolkit. ICRC. 2015.

Cash Transfer Programming in Emergencies: Good Practice Review. Overseas Development Institute (ODI) Humanitarian Policy Network (HPN). June 2011.

Doing Digital Finance Right. CGAP. June 2015.

Policy on the Protection of Personal Data of Persons of Concern to UNHCR. UNHCR. May 2015.

Professional Standards for Protection Work. ICRC. 2013 Edition.

Protecting Beneficiary Privacy: Principles and Operational Standards for the Secure Use of Personal Data in Cash and E-transfer Programs. CaLP.

The Electronic Cash Transfer Learning Action Network is convened by Mercy Corps,
with support from the MasterCard Center for Inclusive Growth.

MERCY CORPS

MasterCard

MasterCard Center
for Inclusive Growth

elan
The Electronic Cash Transfer
Learning Action Network