elan
The Electronic Cash Transfer
Learning Action Network

A DATA STARTER KIT
FOR HUMANITARIAN FIELD STAFF

Learn why and how to manage and protect your e-transfer program data.

Nigeria - Vincent Triysseau/CaLP

TABLE OF CONTENTS AND INTRODUCTION

CONTENTS

INTRODUCTION

When we implement e-transfer programs, we collect a lot of information about program participants, some of which is highly sensitive. So, we have a responsibility to utilize, share, store and dispose of it securely.

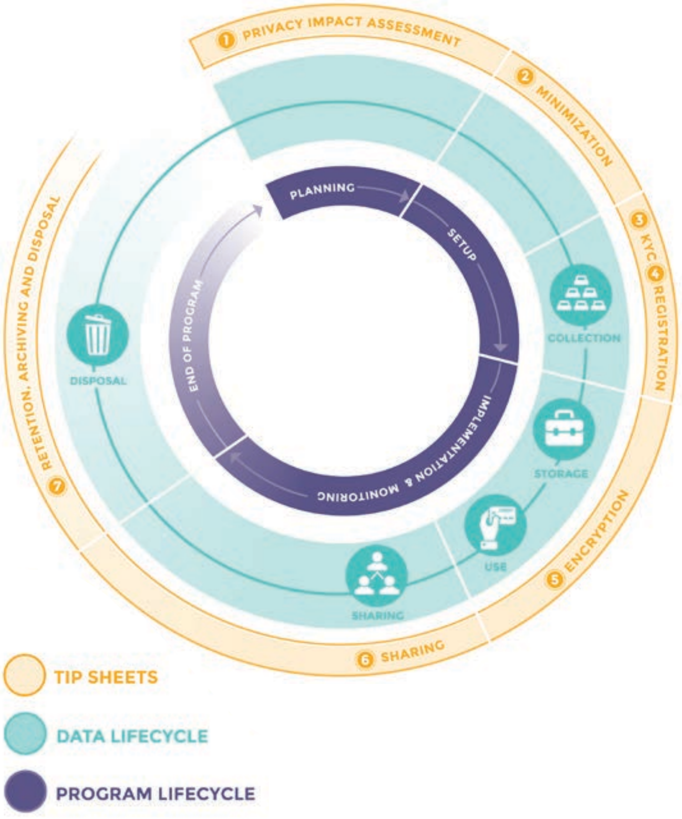
Many industries are governed by clear data protection standards. This is not yet the case for ours. Very few humanitarian organizations have a comprehensive set of policies, practices and tools to responsibly manage and protect the data they hold.

So we put together some tips to get you started. (You're welcome.)

Building upon the Cash Learning Partnership's (CaLP's) foundational *Protecting Beneficiary Privacy*, this Starter Kit provides concrete tips to help you assess, plan and improve your data management practices. The seven Tip Sheets align with the project and data management lifecycles, so you'll know exactly when to think about RAD, PIAs and E2EE.

We developed this Starter Kit for field staff implementing e-transfer programs, but there's no reason to keep it secret. If you think other teams – or other programs entirely – may find the guidance useful, pass them on!

HOW DOES DATA MANAGEMENT FIT WITH MY PROGRAM?



DATA MANAGEMENT AND PROTECTION STARTER KIT

TIP SHEET ①

PRIVACY IMPACT ASSESSMENT (PIA)

WHAT IS A PRIVACY IMPACT ASSESSMENT (PIA)?

A Privacy Impact Assessment (PIA) is a systematic analysis of the potential privacy risks related to data collected during program implementation. A PIA analyzes threats and risks to program data, including any legal and environmental factors, and develops mitigation strategies. PIAs help humanitarians protect participants' privacy and strengthen public confidence in the program.

WHAT HUMANITARIANS NEED TO KNOW:

A PIA should be conducted before data collection starts - usually during a program's planning or inception phase – so that any potential problems can be proactively addressed. Alongside identifying privacy risks, the PIA exercise can be useful in raising overall data privacy concerns between the implementing organization(s), partners, and program participants.

All PIAs should take contextual elements into account; as such, risk assessments may look very different in different country contexts, even if programs themselves are similar. Depending on the sensitivity of the data your program will be collecting, you may want to consider working with an external privacy assessment specialist.

As stated in the Cash Learning Partnership (CaLP) *Protecting Beneficiary Privacy: Principles and Operational Standards for the secure use of personal data in cash and e-transfer programs* *(page 11)*

- *Identify the privacy risks to individuals*
- *Identify the privacy and data protection compliance liabilities for the organization*
- *Protect the organization's reputation and instill public confidence in the program*
- *Ensure that the organization is promoting human rights in its humanitarian activities*

WHAT HUMANITARIANS CAN DO:

SELECT OR ADAPT PIA GUIDANCE

The following steps are adapted from *suggested guidance* from the Privacy Commissioner of New Zealand; please adapt them to fit your individual organization. You may also find CaLP's *Model Privacy Impact Assessment* helpful (pages 19-20). For more detailed guidance, please refer to the "Additional Resources" section at the end of this Tip Sheet.

Step 1: Review your program

Describe your program objectives and activities and outline the different types of data that will be collected, as well as the rationale for collecting this data. Specifically note where personally identifiable information (PII) is collected and used throughout the program since many risks relate to this data (see step 3). Within this list, indicate which data will be collected directly by your organization and which data will be collected by a partner (e.g., participants' transactions records held by a financial service provider). Include details about how and with whom program data will be shared and/or published. Include the cultural context in the description, if relevant.

Draw an information or data lifecycle to highlight the individual data steps, indicating what will happen at each step, who is involved, and how information is transferred between users or organizations.

Step 2: Educate yourself about relevant privacy regulations

Be sure to understand which regulations apply to the data you will be collecting and compare your planned programmatic steps against the legally-established privacy principles of the relevant jurisdiction(s). *(See Know Your Customer—KYC—Tip Sheet.)* Be aware that you might need to take into account multiple regulations (e.g., the location where data is collected, where the data is sent, and/or the legal home of relevant organization(s) or partner(s), as well as donor regulations). In addition to national regulations like KYC, regional or international agreements may also apply.

Alongside legal privacy regulations, include your organization's privacy principles and ethical guidelines in your analysis. If your organization has not developed these, use CaLP's as a starting point. After completing this process for your first e-transfer program, it will become easier to check for updates and adapt this review process for future programs.

Step 3: Identify any privacy risks

Compare the steps you outlined in the data lifecycle (Step 1) against any relevant privacy regulations (Step 2). Based upon regulatory guidelines, are there any differences between how you plan to manage data and how you should be managing data? Think carefully about who might try to improperly use each type of data, how they could gain access, and what would happen if they were successful.

Step 4: Evaluate and mitigate risks

Using the list you established in Step 3, prioritize which are the biggest risks to your data and their likelihood of occurrence. Keep in mind that low-likelihood risks that are potentially damaging should not necessarily be de-prioritized. Use this analysis to identify particular weaknesses in your program plans that need to be addressed. Then, identify mitigation strategies in response to those risks. As you develop mitigation strategies, make sure to include all of the people involved in these different program stages (i.e., field and M&E officers, finance team members) to ensure feasibility of the strategies you develop.

Example risk: An e-transfer service provider enables your NGO to restrict access to PII within the backend platform. However, if the PII contained in the system is exported to an Excel spreadsheet and saved on a shared drive, these restrictions no longer apply, since all staff now have access to the data.

Example mitigation strategy: Restrict the permissions to export data and include guidance in Standard Operating Procedures (SOPs) on securely storing exported information.

Step 5: Draft an accessible PIA report

Clearly document the risks, potential impacts and mitigation actions in your PIA report, since program staff will refer back to this document throughout program implementation. Be explicit about how often this report should be consulted, and whether a formal review of the PIA should be conducted during the program. There is not standard guidance about how often a PIA should be reviewed, but a good rule of thumb is to conduct a review on an annual basis.

Draft the PIA report using simple, accessible language so it can be easily understood by all staff and include definitions of any technical terms *(or link to the Starter Kit Glossary).* If your PIA is particularly long, consider drafting a short Executive Summary to highlight the main decisions that were made based on the assessment. Also, think about how you can structure or present the information in an easily-digestible format (e.g., matrix, data lifecycle diagram) and any needs for translation into a local language.

Step 6: Make an action list

Based on your PIA report or summary, develop a list of concrete tasks and conditions that are required for the PIA to be effective. For example, identify who needs to be made aware of the report, which new tools need to be substituted for less secure ones, what revisions to program plans or SOPs are required. Build the risk-mitigation measures identified in the PIA into your SOPs, and periodically review the effectiveness of these measures.

Step 7: Compare PIAs at the end of similar programs

If similar risks are present in multiple PIAs, it might be a sign that new policies need to be adopted at a higher level to address these risks. Assign a person or a team to cull through PIAs to identify commonalities to inform country or organizational practices.

GET THE MOST OUT OF YOUR PIA

Keep track of your formats and be ready to adapt based on your assessment findings

The most important data sets in e-transfer programs are those that contain program participants' PII. Your organization may hold parts of this data in different formats. When you identify these sensitive data sets and mitigation strategies through your PIA, make sure to apply these strategies to all versions or portions of the sensitive data set.

Adapt based upon your findings

Thinking through your risks and their likelihood (also known as your threat model) may highlight some gaps in your program design. You may need to hire specialists to assist with developing mitigation strategies for these threats or adjust your program plans to respond to identified gaps.

ADDITIONAL RESOURCES:

Privacy by Design. UK Information Commissioner's Office. A component of its overall guide to data protection, this section includes an explanation of privacy by design, the importance of PIAs, and a *code of practice for carrying out a Privacy Impact Assessment.*

Model Privacy Impact Assessment. *Protecting Beneficiary Privacy: Principles and Operational Standards for the Secure Use of Personal Data in Cash and E-transfer Programs*. CaLP. Annex 1, pp. 19-20.

Privacy Impact Assessments. US Government Federal Trade Commission (FTC). A list of publicly-available PIAs drafted for different programs and projects of the FTC. The text itself is not particularly relevant for the cash transfer world, but the assessments are good examples of sector-specific PIAs.

Privacy Impact Assessment Toolkit. Privacy Commissioner's Office in New Zealand. Templates and checklists to help construct a PIA and choose which elements to include.

McDonald, Sean. *Ebola: A Big Data Disaster: Privacy, Property and the Law of Disaster Experimentation*. CIS Papers. January 2016. A general piece about the complexity of potential legal risks and liabilities when humanitarian organizations capture PII.

DATA MANAGEMENT AND PROTECTION STARTER KIT

TIP SHEET 2

DATA MINIMIZATION

WHAT IS DATA MINIMIZATION?

Data minimization is a privacy principle that requires the people collecting data to be intentional about what type of data is collected and how long it is retained. To meet this principle, teams should limit data collection to what is directly relevant and necessary to accomplish a specified purpose. In practice, this means assessing whether personally identifiable information (PII) must be a part of a data set and how long to keep data before disposing of it. Data minimization also refers to de-identification practices in which PII is stripped out of data sets before they are shared with others or made accessible to the public.

Data minimization applies to most program phases. Collecting the minimum amount of data, sharing only with those who need it, and keeping data only as long as necessary has clear privacy advantages; the less you have and the quicker you dispose of it, the less likely data can be inadvertently disclosed. But data minimization also has financial advantages; organizations spend less time and money collecting unnecessary data, cleaning it up once collected, and storing and archiving excess data.

Programs should strive to maintain a balance between responsibly minimizing data, while ensuring that data collection meets program needs.

Regulations and guidelines

There are few legal regulations that govern what type and quantity of data you can collect, but there are guidelines which can assist in making decisions related to data minimization.

One, the *OECD Privacy Principles*, states:

> *There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.*

Another, the *Fair Information Practices Principles*, (FIPPS) states that:

> *Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).*

Data minimization is also addressed under the Cash Learning Partnership (CaLP) Principles and Operational Standards:

Principle 4: *Organizations should ensure the accuracy of the personal data they collect, store and use, including by keeping information up to date, relevant and not excessive in relation to the purpose for which it is processed, and by not keeping data for longer than is necessary.*

Principle 7: *Organizations should not hold beneficiary data for longer than is required unless they have clear, justifiable and documented reasons for doing so, otherwise data held by the organization and any relevant third parties should be destroyed.*

WHAT HUMANITARIANS NEED TO KNOW:

Understand what constitutes PII

To minimize the collection of PII, it is important to understand exactly what it is. Simply put, PII is, “Any data that directly or indirectly identifies or can be used to identify a living individual.” Names, phone numbers, bank record details, and biometric data (such as fingerprints or iris scanning) are all common examples of PII. However, PII can also be any combination of data sets (sometimes seemingly innocuous ones) that would allow someone to identify an individual. Since e-transfers are typically distributed to an individual or household, e-transfer programs tend to require PII to be able to target assistance and ensure assistance is received by the correct participant.

Consider the privacy rights of your program participants

Emerging technologies are revolutionizing the way humanitarians can collect, collate and communicate data. While these changes can positively impact planning and program efficiency, it is essential to evaluate whether data is being collected with a view to the privacy rights of program participants. *(See PIA and Registration Tip Sheets for more information).* Possible questions to ask when collecting data are:

- Have you clearly explained how the data will be used and requested program participants' consent?
- If it is not possible to get consent, what have you done to protect participants' data privacy rights?
- Do participants know who will have access to their data?
- Do participants have access to their data, and can they change their minds about giving you access to you later in the program?

Why practice data minimization?

Risk to individuals: The risks of not adequately thinking through data minimization are serious, particularly because of the conditions that individuals and communities face in humanitarian situations. Be realistic. Data breaches happen, and collecting excessive PII increases the chances those breaches will cause harm. Data breaches can have many negative consequences for individuals, such as denial of services or freedoms, fraud and identity theft.

Reputational risk: The use of digital data gathering (DDG) solutions in humanitarian programs is increasing, including biometrics for registration and verification. Much of this technology was not designed for the humanitarian sector. Instead, it was adopted from sectors and not necessarily developed with the communities in which we work in mind. In addition to potential harms to data subjects, privacy breaches and insider leaks can be damaging to the reputation of a humanitarian organization. Practicing data minimization and access minimization (minimizing the number of people with access to sensitive data) mitigates the risk of this happening.

Time and cost-efficiency: Collecting only necessary data minimizes time spent by program participants, collectors, data cleaners, and processors. Conducting a proper assessment of what kind of data you need to collect, who will access it, and how long it should be kept will increase your program's data security. It will also increase your ability to share data later on, if necessary. *(See the PIA and the Data Sharing Tip Sheets for more information.)*

WHAT HUMANITARIANS CAN DO:

While it is tempting to collect as much data as possible in the off-chance that you might need it later, you should resist this temptation. Particularly for humanitarians working with vulnerable groups, there are risks associated with collecting unnecessary data. To meet the principle of data minimization, use the other Tip Sheets in this Starter Kit to help you determine your scope of data collection and retention.

- **Responsible data collection and use:** Think about what data you need for the project (and collect only that information). *(See PIA and Registration Tip Sheets for more information).*
- **Responsible observance of data regulations:** Think about the host country data laws. *(See KYC Tip Sheet for more information.)*
- **Responsible data access and sharing:** Think about who needs to access the data collected and with whom you are required to share it. *(See Data Sharing Tip Sheet for more information.)*
- **Responsible data storage/retention:** Think about how long you'll need to use the data (and keep it only for that length of time). *(See Retention, Archiving and Disposal Tip Sheet for more information.)*

ADDITIONAL RESOURCES:

Anonymisation Decision-Making Framework. UK Anonymisation Network. An interactive guide.

Privacy Principles. Organisation for Economic Co-operation and Development (OECD).

Fair Information Practice Principles. National Strategy for Trusted Identities in Cyberspace, Appendix A. National Institutes of Standards in Technology (NIST).

Professional Standards for Protection Work. ICRC. 2013 Edition.

Anonymisation: managing data protection risk. UK Information Commissioner's Office (ICO). A summary of an anonymisation code of practice.

Hansen, Marit and Andreas Pfitzmann. *A terminology for talking about privacy by data minimization: Anonymity,Unlinkability, Undetectability, Unobservability, Pseudonymity,and Identity Management*. August 2010.

DATA MANAGEMENT AND PROTECTION STARTER KIT

TIP SHEET 3

KNOW YOUR CUSTOMER (KYC) REGULATIONS

WHAT ARE KNOW YOUR CUSTOMER (KYC) REGULATIONS?

Know Your Customer (KYC) regulations, also known as customer due diligence, are designed to combat money laundering, terrorist financing, and other related threats to the financial system. They refer to the ID checks that financial institutions perform to comply with national financial regulations. Typically, KYC checks take place when customers sign up for an account or conduct a transaction. However, KYC checks can also occur during events less visible to customers, such as creating customer transaction models and monitoring for unusual activity.

Humanitarian agencies are not directly subject to KYC regulations. However, the financial service providers (FSPs) they often partner with are. KYC regulations apply to FSPs whether they are based within or outside the country of implementation. FSPs must comply with them or face fines and penalties. As a result, FSPs apply policies designed to meet KYC regulations for all clients, including humanitarian organizations and their program participants, and tend to be risk-averse.

KYC requirements are set at the national level and may vary depending upon specific criteria. This criteria might include what type of FSP is involved (e.g., remittance companies, banks, mobile network operators, etc.); the transfer value; the account ceiling or the product itself. Differences between these tiers or types of applicable regulations can have significant implications for humanitarian programming.

WHAT HUMANITARIANS NEED TO KNOW:

- Know what type of ID the FSP requires from program participants to receive cash, establish accounts or access other services.
- Be aware of regulatory differences that may apply to different providers, services or transfer amounts.
- Understand who will be collecting KYC information (e.g., the humanitarian organization or the FSP) and know how it will be shared and stored. Clarify which teams will check the collected information and correct errors.
- Be aware of your FSP's obligations or procedures around the disclosure of KYC information to host or donor governments or other companies.
- Understand your host country's past experience. In the event KYC regulations were relaxed, under what circumstances did this take place, how quickly and for what length of time?
- Keep in mind that refugees often face KYC-related challenges to accessing financial services or establishing accounts since they frequently lack IDs issued by host country governments or other documentation to meet KYC requirements.

Where you foresee challenges in meeting KYC requirements, discuss alternative arrangements immediately with your selected FSP or raise them with relevant authorities. If no solution can be found, you may need to pursue an alternative transfer mechanism to provide assistance.

When you plan with your selected FSP, take into account KYC requirements in setting responsibilities and systems for providing informed consent, collecting and storing KYC information, and in planning data protection and sharing measures, where required. *(See Registration, Encryption, Sharing, and Retention, Archiving and Disposal Tip Sheets.)* For example, if the program creates accounts for participants and the agency and FSP want to support continued use of these accounts, the agency and FSP should plan from the early stages to secure informed consent to share the required KYC information.

WHAT HUMANITARIANS CAN DO:

Know your operating context

The first step to address KYC regulations is to learn which apply in your country of operation. As part of your assessment of cash feasibility and delivery mechanisms, gather information on FSPs' KYC policies. FSPs may also be able to share information about national KYC requirements. Keep in mind, however, that FSPs may differ in their interpretation of national KYC requirements (or may have company compliance requirements that are more stringent than national requirements). Knowledge about national KYC requirements can help you troubleshoot and modify programs to speed start-up (for example, by providing a program participant photo ID as an identity document). Online global guides to KYC regulations summarize the key points of some countries' national legislation.

SAMPLE QUESTIONS FOR YOUR FSP:

- What are your normal KYC requirements and process for verifying IDs?
- Is there a transfer amount below which KYC requirements do not apply, additional identification requirements that apply above a certain transfer amount, or other differences in requirements based on type of service?
- Can you offer transfers to multiple program participants through a single agency account?
- How do you collect and store program participant information?
- What are you legal obligations to disclose customer information to authorities?

KYC regulations apply to third-country FSPs

When selecting an FSP outside your country of operation, make sure they have the knowledge and experience to address KYC requirements in your country of operation to avoid delays.

Know your program participants

Consider whether factors such as refugee status, mobility and possession of IDs will affect participants' ability to establish accounts. When selecting the best transfer option for you program, consider whether sensitivities or persecution could mean that gathering KYC information would place populations at risk. *(See PIA Tip Sheet for more information.)*

Evaluate account options

Organizations should consider the potential tradeoffs related to KYC requirements for different account options. For example, if simplified KYC requirements are available for a limited time or for accounts with a lower ceiling, selecting these options could speed distribution. However, these choices could limit participants' ability to access the features of a full account or may require additional data collection later. Evaluate benefits and tradeoffs against other factors, including the number of participants your program will serve, the program's duration and objective, staff time required for contracting and data management, and other pertinent criteria.

Explain KYC requirements to program participants

National KYC regulations may dictate that FSPs routinely share customer information with national authorities. If this is the case in your country of operation, make sure participants understand this use of their data before data collection begins. *(See Registration Tip Sheet for more information.)*

Advocate for adjusted KYC regulations

While potentially time-consuming, some responses may call for a temporary adjustment of KYC regulations for affected populations. In the case where national regulations are a significant barrier to timely delivery of electronic assistance – particularly where many people have lost ID documents – you may want to work through coordination bodies, such as a Cash Working Group, to advocate for temporary adjustments to KYC regulations. Adjustments could include accepting additional types of ID, issuing temporary IDs, or allowing participants to open new accounts with a grace period in which they provide ID documents. (Specific examples of adjusted KYC regulations are covered in the next section.) In countries prone to natural disasters, cash coordination bodies could undertake these discussions as a preparedness measure.

Share your insights

KYC regulations are nationally applicable and information gathered from particular FSPs can benefit others. Share your findings with Cash Working Groups to avoid posing duplicative questions to FSPs.

EXAMPLES OF ADJUSTED KYC REGULATIONS:

Below, are examples where dialogue between FSPs, national regulators, program participants and humanitarian agencies helped to structure or adjust KYC regulations during humanitarian responses.

- In the **Philippines**, authorities temporarily waived ID requirements for transactions in affected areas, enabling people who lost ID documents during Typhoon Haiyan (Yolanda) to access cash assistance. Limits were set on the transfer amount participants could accept and they were required to document in writing that their ID had been lost.
- In **Haiti**, where mobile money was launched after the 2010 earthquake and designed with affected peoples' needs in mind, KYC requirements vary based on the ceiling of the mobile wallet. A mini wallet with a ceiling of approximately US$85 in transaction value does not require the holder to provide a national ID. A full wallet with a higher ceiling requires in-person registration in a bank branch with national ID documents and the applicant's signature.
- Overseas banks holding the accounts of **Somali** money transfer operators feared significant penalties under home countries' regulations, since it was difficult for them to verify the identity of the end recipient of remittances. These banks have closed many of the Somali money transfer operators' accounts, compromising significant volumes of remittance and humanitarian transfers into Somalia. Humanitarian agencies have helped advocate for clarity in international regulations so that money transfer operators can continue offering services to Somalis and humanitarians, since these funds represent a critical source of support for families and agency operations.
- **Nigeria** offers a three-tiered KYC requirement regime for low-, medium- and high-value accounts. Low-value accounts have a limited single deposit amount and maximum allowable cumulative balance, but require limited information to open an account. Medium- and high-value accounts require additional documentation to prove identity.

CHANGING INTERPRETATIONS AND DEVELOPMENTS:

Research on KYC regulations in humanitarian contexts suggests some developing interpretations that could affect humanitarian agencies and FSPs' collection and use of KYC information. Scholars have argued that the humanitarian agency, rather than the program participants, should be the singular customer subject to KYC requirements (rather than each individual participant), since the agency holds the contract with the FSP. If this view were to become more widely accepted, it could tremendously simplify KYC considerations in humanitarian programs. Ideally, researchers have suggested a standardized, simplified set of KYC requirements applied in all humanitarian emergencies; however, this is far from reality right now.

ADDITIONAL RESOURCES:

di Castri, Simone. *Mobile Money: Enabling regulatory solutions*. GSMA Mobile Money for the Unbanked. February 2013.

Keatinge, Tom. *"Counter-terrorist regulation restricts charity banking worldwide..." Uncharitable Behaviour*. Demos. 2014.

Know Your Customer: Quick Reference Guide. PricewaterhouseCoopers. January 2014.

Levin, Avner, Anupa Varghese, and Michelle Chibba. *Humanitarian Cash Transfer Programs and Beneficiaries: Know Your Customer Standards and Privacy Recommendations*. UNHCR. 2015.

Metcalfe-Hough, Victoria, Tom Keatinge and Sara Pantuliano. *UK humanitarian aid in the age of counter-terrorism: perceptions and reality*. HPG Working Paper. 2015.

Pantuliano, Sara, Kate Mackintosh and Samir Elhawary. *Counter-terrorism and humanitarian action*. Overseas Development Institute: Humanitarian Policy Group. 2011.

Smith, Gabrielle. *Electronic Transfers Scoping Study and Preparedness Plan*. ACF Philippines. December 2013.

Smith, Gabrielle. *Cash coordination in the Philippines: A review of lessons learned during the response to super Typhoon Haiyan.* Cash Learning Partnership and UNHCR. March 2015.

DATA MANAGEMENT AND PROTECTION STARTER KIT

TIP SHEET 4
REGISTRATION

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.

DATA MANAGEMENT AND PROTECTION STARTER KIT

TIP SHEET 5

ENCRYPTION

WHAT IS ENCRYPTION:

Encryption uses complex mathematical algorithms to encode information, making it unintelligible to anyone without the key to decrypt it. Encryption is designed to protect sensitive information. Once encrypted, information can safely pass across public networks, like the Internet, without being stolen.

For ease of use, systems are often set up to automatically encrypt information before sending and to automatically decrypt information received.

Bear in mind that while encryption reduces risk, it does not eliminate it. Encryption is continuously evolving and previously secure methods are regularly broken. Using encryption makes it more difficult for unintended users to access your data, but it does not provide absolute security, particularly against sophisticated adversaries.

The first step to protecting sensitive information is to reduce how much of it you collect and keep. *(See Data Minimization Tip Sheet for more information)*. Unless you have a good reason to store a particular file, or a particular category of information within a file, you should delete it. *(See Retention, Archiving and Disposal Tip Sheet for more information.)* The best option to protect sensitive information is to not hold it to begin with. The next best option is encryption.

WHAT HUMANITARIANS NEED TO KNOW:

Data at rest vs. data in transit

When considering encryption, it is important to understand the two states in which data can exist. Data can be stored somewhere, or it can be passed between users. Stored information (e.g., a file on a laptop) is called "data at rest". Data that is being passed around (e.g., an email sent across the Internet) is called "data in transit".

If data at rest is encrypted, an attacker who steals your information will not be able to read it. If data in transit is encrypted, eavesdroppers will not be able to understand it.

For data collection in remote locations, without electricity or internet connection, data is often physically transported by program participants and humanitarian field staff (e.g., on mobile phones or physical paper files). Data on mobile phones is an example of both data at rest and data in transit. To make sure this data is safe, you will need to consider both how the data is stored on the phone (data at rest) and how it is transferred from the phone (data in transit).

Trusted vs. untrusted

It is also important to consider where data at rest is stored and where data in transit is passed. Is your information stored in a "trusted" location, such as an office file-server, or is it stored in a public and therefore "untrusted" location, such as a public DropBox or Google Drive folder?

These same considerations apply to data in transit. Is your data passing through private and trusted networks, such as a file being printed from your laptop across your office network to an office printer? Or is it passing through an untrusted, public network, like an email from you to a colleague at another organization, which passes through the Internet?

To be effective, everyone must use encryption

Encryption is a powerful method of increasing security, and can be used to mitigate many of the risks to PII data when adopted program-wide. However, your data is only as secure as the weakest link in your program. If even one person fails to use encryption, your program data is at risk. This means that encryption is not just a question of technology: it requires a commitment to changing behaviors as well.

Encryption software and national legislation

Laws in some countries (such as Sudan, Yemen and Pakistan) place limits upon the nature of encryption software allowed for the communication and storage of data. Before using encryption, ensure either that it is legal to do so in your country of operation or that you understand the legal risk. Currently, there is little guidance on the global status of encryption laws, so this will require a country-by-country analysis.

WHAT HUMANITARIANS CAN DO:

Use your Privacy Impact Assessment (PIA) to determine which data should be encrypted

To understand which data needs to be encrypted, review the risk analysis from your PIA, which outlines the nature and type of data your program is collecting. Then ask:

- Does my data include personally identifiable information (PII)?
- Are there risks associated with disclosure of this data (or could there be in the future)?
- Are the communities/groups described by this data “vulnerable”?
- Is there extensive government control of mobile communications and/or widespread surveillance of phone and internet connections?
- What are the political, religious, ethnic or social contexts in the country which might create particular risks when collecting and using personal data?
- What are the security vulnerabilities of the technologies and tools we are using to collect, store and transfer data?

Think about encryption early in your program

Using your PIA, assess the risks to your data and consider the various encryption tools available to you (outlined below). Make sure to budget for the time and resources necessary to incorporate encryption practices into your program. Once you have selected a technology, train team members during the planning stages of your program. Encryption practices should then be adopted during the collection, storage and transfer of PII and sensitive program data.

Encrypting data at rest

There are three main strategies to encrypt data where it is stored. Before you encrypt any data, see if there is anyone in your organization who is an encryption expert, who has tried encryption before or who is interested in trying it now. It is always helpful to have someone to troubleshoot with as you are trying out new processes for the first time.

1. **Encrypt the drives on your device (laptop, phone, tablet):** All modern operating systems (Mac, Windows, iOS, Android) have built-in encryption that will encrypt all data stored on the device. With encryption turned on, if someone steals your device, they cannot read the contents without your password or passcode. Without encryption, a hacker can easily access the contents of your device.

To turn on encryption on your devices:

- For Windows computers, use the built-in *BitLocker feature*.
- For Mac computers, use the built-in *FileVault* feature.
- For iPhones and iPads, simply *set a passcode* and the system will automatically encrypt the phone.
- For Android phones and tablets, *these instructions* explain how to turn on encryption.

2. **Encrypt individual files or groups of files:** Using archive software such as *WinZip* (Windows, Mac, Android, iOs) and *7-Zip* (Windows and Linux), you can place a file or folder – or set of files and folders – in an archive file format that is compressed and encrypted. To view the files, open the archive with the archive application and enter the password to extract the original files.
3. **Create a "virtual" encrypted disk:** VeraCrypt *(see this guide for more information)* and similar software will create virtual encrypted disk drives to hold files. VeraCrypt automatically encrypts data right before it is saved to an encrypted drive and decrypts it right after it is loaded. No data stored on a VeraCrypt encrypted drive can be read without using the correct passphrase or encryption key.

Encrypting data in transit

When data is moving from one computer to another, encryption acts like a lockbox to keep the data you are sending private and secure.

Data in transit over the Internet (including VOIP applications like Skype) can be encrypted using the methods outlined below. However, data transferred over SMS or GSM voice channels cannot. As such, mobile phones have certain risks inherent to their use. For more information on how to use mobile phones securely, see *this guide* from security in-a-box.

- **Http Secure (https):** The first five letters of most urls – https – is a protocol for secure, encrypted online communication. In contrast to http, https provides authentication of the website you are visiting, which protects against *man-in-the-middle attacks*. It also prevents eavesdropping and tampering with the contents of online communication between the user and the website. To prevent webpages from defaulting to http (and making you vulnerable to attacks and eavesdropping), you can install a browser plugin called *HttpsEverywhere*, which defaults web pages to https.

- **Encrypt individual files**: Encrypting individual files before sending them via email is a quick-and-dirty way to achieve encryption in transit. (See "data at rest" section above.)

- **End to end encryption (E2EE)** systems are digital systems that facilitate secure, encrypted communication over "untrusted" third party connections, such as Internet providers or application service providers. Your data is encrypted locally on your device before being sent across a network or to a server to be stored, and therefore cannot be read by third parties.

  Ideally, your organization would use E2EE for all internal communications, as well as communications with partners and other third parties. (The "tools" section below includes examples of E2EE communication services.) If you do not use E2EE tools, you can encrypt files or groups of files and send these encrypted versions to your partners. To utilize this approach, you will need to provide them with the passphrase or decryption key through a separate communications channel. (In other words, do not email the encrypted file and passphrase together.)

  Also, in an ideal setting you could use applied E2EE, which involves exchanging encryption keys with those with whom you wish to communicate. However, these tools require a more intensive set-up process for both sides that is likely impractical for field staff communications. If you are interested in setting up these systems, reach out to your IT team for assistance.

Archiving Data

As a reminder, encryption does not protect your data from being lost, since an encrypted file can be deleted like any other file. Best practice is to archive data often, and to ensure that any sensitive data is archived in an encrypted form, particularly when it sits with a third party service provider. *(See Data Retention, Archiving and Disposal Tip Sheet for more information.)*

Other tools to reduce risks to your data

Encrypting program participant information or other sensitive data can decrease the risk of disclosure or misuse of data at rest and in transit. But what about other risks? Below are best practices to reduce the vulnerability of your online accounts and computer.

- **Create strong passphrases** and protect them with a password manager such as *KeyPass*. A password manager will generate new, secure passphrases for each service requiring one. These passphrases are then encrypted and can only be accessed using one, very secure passphrase - the only one you need to remember. Also, change your passwords regularly. For more information, see *this guide to downloading and using KeyPass* from Tactical Tech.

- **Two factor authentication (2FA)** prevents someone who has gained access to your passphrase from accessing your account. To get into your account, 2FA requires that you have both “something you know” (a strong passphrase) and “something you have” (such as your phone). After you enter your passphrase, a code will be sent to your phone. You can only access your account after entering this code. See this extensive *list of websites* that support 2FA.

  Caution: Be aware that strong passphrases and 2FA only help decrease the risk of someone accessing protected accounts. They do not protect data at rest on a USB drive or computer that is physically stolen or from an Internet service provider reading your unencrypted traffic.

- **Restrict who has access** to sensitive data through role-based administration and password protection.

- **Check the track record** of your private sector partners regarding data protection and privacy.

- Ensure that **transfers of personal data** within and between organizations are **only undertaken when required** as a program imperative, are done through secure means, and that the recipients of the data will in turn recognize its confidential nature. These steps can be included in a data sharing policy. *(See Sharing Tip Sheet for more information.)*

ADDITIONAL RESOURCES:

Resources

The Hand-Book of the Modern Development Specialist Responsible Data Forum. Provides an overview of some encryption strategies.

Surveillance Self Defense. Electronic Frontier Foundation. Includes useful introductions to some of the tools and concepts outlined here.

Journalist Security Guide. Committee to Protect Journalists. In-depth guide (aimed towards journalists, though still relevant for humanitarians) to data security throughout the project timeline.

SURVEILLANCE AND COUNTER-SURVEILLANCE For Human Rights Defenders And Their Organisation. Protection International. December 2014.

Data Integrity Guide. FrontlineSMS.

Technical Tools

Data at rest

WinZip, *7-zip*, and *VeraCrypt*: software to encrypt files on your computer, USB stick or external hard drive.

KeePass: an application on your computer that manages and stores encrypted passwords (see *security in-a-box guide*).

Data in transit

Automatic E2EE services:

Jitsi: Secure instant messaging (IM), voice and video chat over the internet (see *security in-a-box guide*).

Pidgin + OTR: Secure IM (see *security in-a-box guide*).

Signal: Secure calls and chat.

Note: *If using any these services, make sure to involve your IT department for installation assistance and training.*

Secure browsing

HttpsEverywhere: a browser plugin to default web pages to https to help prevent *man-in-the-middle attacks*, when someone eavesdrops on and tampers with the contents of the site and the information you send to the site.

DATA MANAGEMENT AND PROTECTION STARTER KIT

TIP SHEET 6

RESPONSIBLY SHARING DATA

WHAT IS DATA SHARING?

Data sharing is the ability to share the same data resource with multiple applications or users. In e-transfer programs, data about program participants is often shared with financial service providers (FSPs) and/or governments for programmatic and regulatory reasons. This Tip Sheet explains the different types of data sharing, the technical means by which data is shared and strategies for responsibly sharing data.

WHAT HUMANITARIANS NEED TO KNOW:

Collaboration with other stakeholders is a key aspect of many humanitarian projects. In e-transfer programs in particular, humanitarian organizations frequently share program participants' personal data with FSPs. Where required, personally identifiable information (PII) may also be shared with host country governments. This personal data may include names, telephone or ID numbers and even biometric data. As such, it is important to plan for responsible data sharing to mitigate the risk to program participants that their PII is misused.

The expectations for organizations related to responsible data sharing is sprinkled throughout the CaLP Principles and Operational Standards, including:

Principle 2: *Organizations should "protect by design" the personal data they obtain from beneficiaries either for their own use or for use by third parties for each cash or e-transfer programme they initiate or implement.*

Alongside PII, FSPs are often the primary custodians of transaction records, which provide a record of where and when people made purchases, as well as information about their savings and spending habits. This transaction data, while not inherently sensitive, should be protected as it could be misused. Therefore, it is important to both understand what data you require from FSPs as well as obtain a clear picture of data they will gather about your program participants while providing their services.

WHAT HUMANITARIANS CAN DO:

Adhering to responsible data sharing is an ongoing practice, since data is shared throughout the program lifecycle. To make sure you create the right types of data sharing agreements, begin by understanding with whom you will be sharing data. Sometimes this is referred to as types or "levels" of data sharing. Data sharing may often involve multiple types or levels. Below are listed four common types of data sharing, as well as relevant considerations.

- **Internal data sharing:** Data shared within an organization. Even if managing internal permissions falls outside your role, be aware that people in your organization beyond your immediate team may have access to the places where your program data is stored (e.g., your internal intranet). If you are not sure about who has access to internal systems, it may be worthwhile to speak to your IT team to gain an understanding of permission levels and make sure you store data where the right people can access it.
- **Sharing data with known partners:** Data shared with coordination partners. In this scenario, you do know all actors who need access to the data. Depending upon your partners, you might choose to develop separate data sharing agreements with private sector and humanitarian partners.

- **Sharing data with unknown partners**: Some donors or private sector partners—such as banks—may by default make their data available to other partners, of whom you may be unaware. (See data sharing agreements below for ways to limit sharing with unknown partners.) Data shared with one government body may also be shared within other government bodies.
- **Publishing data:** Making program data public. Publication can happen in response to a requirement from a donor, for example to adhere to aid transpare

Ensure that data subjects have given their consent

Prior to sharing any kind of data, it is essential to ensure that people reflected in the data ("data subjects", most often your program participants) understand what will happen to their data and have given their informed consent for its use. This means that participants have given their permission for the data to be shared, with full knowledge of the potential consequences. Note that in emergency contexts this may not be possible. *(See the Registration Tip Sheet for more information.)*

Establish a data sharing agreement between partners

It is important to explicitly state what type of things can or cannot be done with data prior to sharing. The best way to do this is to establish a data-sharing agreement framework. If possible, refer to existing agency or company data protection policies. These may be internal policies, particularly if your organization is large, or external policies to share with third parties. Data sharing frameworks do not necessarily contain information specific to the program data you will collecting. Rather, they make explicit the "do's and don'ts" that might come up when sharing data with a range of partners (e.g., local NGOs, international NGOs, FSPs and others), allowing them to apply to a range of programs.

This framework may be referenced or integrated into a:

- Memorandum of Understanding
- Non-disclosure agreement
- Contract

If integration is not possible, you can also create a standalone Data Sharing Agreement.

The *CaLP Principles and Operational Standards* provide a list of very helpful draft clauses that you may want to consider including in your agreement framework for third parties. These draft clauses can be found in **Annex 2** ***(pages 24 to 27)***.

Other examples of these data sharing agreements and resources include:

- DataKind's nondisclousure templates: 1 and 2
- *Key elements of a data sharing agreement* by National Neighborhood Indicators Partnership

Review partners' data sharing policies

When setting up agreements to share data with **private sector partners**, make sure to review their data sharing policies. Some may allow "sharing with third party" as a default clause within their contracts, which is so broad as to essentially encompass any future sharing of your program data. If you are not comfortable with this scenario, make sure to raise the issue in advance of data sharing. It may be well within reason to push back against a default data sharing policy and make access to program data more deliberate. If this is the case, be explicit about data sharing conditions in your contract.

When sharing data with **humanitarian partners**, it may also be necessary to ensure they are aware of issues covered in this Data Starter Kit by sharing relevant resources or providing or recommending training. If these concepts are new, engage colleague agencies in a discussion prior to signing a data sharing agreement to make sure they understand the concepts and have the resources and knowledge to implement the agreement.

With either type of partner, identify a timeline for data sharing to avoid confusion later. Make sure data sharing agreements include this timeline and clearly explain for how long each party needs access to the data. *(See Data*

Retention, Archival and Disposal Tip Sheet for more detailed guidance on archiving.)

Determine what information needs to be shared, and with whom

Data sharing agreements are an important component of responsible data management. In practice, however, there may be little you can do to control how people use or share your data further. For this reason, it is important to adhere to **data minimization** principles when determining exactly what data needs to be shared and with whom. *(See Data Minimization Tip Sheet for more information.)* Share only the required data, rather than entire data sets. Likely, this will mean creating different, redacted versions of data sets for different uses and partners.

Certain types of data, such as PII, should only be shared in extremely rare circumstances. To remove this kind of information, see the *Responsible Data Forum's discussion on de-identifying data*.

Finally, consider how partners need to access the data. Do they need to edit it or simply view it? Depending on the software or technical method used to share the data, you may be able to set access permissions to control data use. (See the table below). Be sure to raise the issue in advance of data sharing. It may be well within reason to push back against a default data sharing policy and make access to program data more deliberate. If this is the case, be explicit about data sharing conditions in your contract.

Within your organization, assign roles and responsibilities

In order to put a data sharing agreement into action, you must clarify the roles and responsibilities of people within your organization who may be involved in handling the data (e.g., staff, interns, consultants and others). Who is responsible for the secure transfer of data to the third party? Who is responsible for minimization and/or de-identification of the data set? Who has access to the data? Who is responsible for securing a data sharing agreement with the third party?

Identify appropriate sharing methods

There are multiple technologies available to share data. You will want to choose one or more methods based upon how sensitive your data is and the levels of access required from those with whom you are sharing data. Some methods include:

Data Sharing Methods and Security Tips

METHOD	SECURITY CONSIDERATIONS	TOOLS, TACTICS, PRACTICES*
Host the data "in the cloud" and share the location with recipient	**Insecure**. With cloud hosting, it is challenging to ensure that the company/companies who own(s) the data servers will protect your data. Utilizing cloud hosting requires users to actively manage permissions of people who at one point needed access to your data, but no longer do. Since these tools often sync automatically to users' computers or other devices, they make data management very complicated since users may retain out-of-date versions even if they are removed from updates or have permissions changed.	• Dropbox • Google Drive • Encrypting the data prior to uploading it could make this option more secure. For example, you could put data in a VeraCrypt volume so that, theoretically, only the intended recipient would be able to access it. *(See Encryption Tip Sheet)*

METHOD	SECURITY CONSIDERATIONS	TOOLS, TACTICS, PRACTICES*
Email *(unencrypted)*	**Insecure**. Depending upon the provider and service, it can be relatively easy for other people to access the message and data when unencrypted email is being sent.	• Email service provider (e.g., Gmail, Hotmail, Yahoo, etc.). • As above, pre-encrypting data and providing the password separately would provide additional security when using this method. *(See Encryption Tip Sheet)*
Physically delivering an encrypted- and password-protected external hard drive, USB stick, CD or DVD	**Digitally secure, but potentially physically insecure**. This method is digitally secure, because you know the recipient is the only person receiving the data and the data is protected in transit. However, this method adds an element of physical insecurity if, for example, the USB stick is lost during delivery.	• If you are working with people in the same location, this may be a good method given how simple it is to implement. • For an extra layer of security, encrypt the data on the hard drive or USB stick, though data deletion can be hard to track if the encryption is broken.
Host the data on an encrypted cloud platform	**Secure**. In this method, access is very limited and data is protected while at rest. Encrypted cloud platforms require the data to be password-protected, protected by SSL during upload/download and encrypted in the location that it is stored. This method can require specific technical capacity to set up.	• *OwnCloud* is a self-hosted service. • *Peerio* is an example of a secure data transfer platform.
Encrypted email	**Most secure** (but difficult). Since the message and data are protected in transit and the recipient is trusted, this is a very secure method for sharing data. It is more difficult to utilize since it requires significant configuration skills on both sides and time to establish. *(See Encryption Tip Sheet)*	• Thunderbird email client + • GPG tools application + • Enigmail plugin • Encrypted email is a best practice in controlled environments, but may be impractical for field use.

** Please note: This is not an exhaustive list of tools or tactics given the short shelf-life and rapidly changing state of many tools. Before pursuing any of these options, please consult with relevant experts in your organization or trusted partners to get the most up-to-date products on the market.*

As you consider what technology is best placed to meet your data sharing needs, it might be helpful to think about worst-case scenarios. For example, if you chose to store something in Dropbox and the information was leaked, would this put people at risk of harm or be particularly damaging? If so, then choose another, more secure method.

For all methods and partners, your goal is to ensure that roles and responsibilities are clear to maintain program participants' privacy.

ADDITIONAL RESOURCES:

Protecting Beneficiary Privacy. CaLP.

De-identifying data

Summaries and recordings of discussion mini-series on de-identifying data

Anonymisation Decision-Making Framework

Introduction to k-anonymity and other de-identification frameworks

Data sharing agreements with third parties

Protecting Beneficiary Privacy: Principles and Operational Standards
Parties. CaLP.

Responsible Program Data Policy

DATA MANAGEMENT AND PROTECTION STARTER KIT

TIP SHEET 7

DATA RETENTION, ARCHIVING AND DISPOSAL

WHAT ARE DATA RETENTION, ARCHIVING AND DISPOSAL?

Data retention refers to the length of time that data is kept by the organization that gathered it. **Data archiving** describes the intentional preservation of data in a format that makes it easy for collaborators to refer back to. And **data disposal** is the process of deleting data in a safe and responsible manner. All are critical to safely and securely managing program data.

WHAT HUMANITARIANS NEED TO KNOW:

Plan from the outset

Although retaining, archiving and disposing of data all occur at the end of the data and program lifecycles, plan for them from the beginning. Leaving these decisions to the end of a program increases the risk that they will become rushed afterthoughts. Without deliberate planning, you may run out of resources or time to responsibly manage this stage of the data lifecycle. This lack of planning can put program participants at risk or cause you to store data longer than necessary.

Understand the needs of all stakeholders

Even within the same program, different teams can have different data retention needs. For example, finance and compliance staff might need to access program data for a donor audit years after a program ends. In contrast, program staff may no longer need data once the program is complete. To meet the data needs of all teams, it is important to reach a shared understanding of each team's data retention needs prior to program end. As such, discuss and plan for data retention needs during program start-up to ensure the systems for collecting and storing program data will link smoothly.

Only retain what you need

Programs often gather a lot of data. For fear of deleting critical data, some program managers may choose to retain all data. Deleting data prematurely does pose an understandable risk (and this is covered more below). Yet, retaining data for too long – particularly participants' personally identifiable information (PII) – is equally risky.

The CaLP Principles and Operational Standards specifically recommend that you retain program participants' PII no longer than required:

Principle 7: *"Organizations should not hold beneficiary data for longer than is required unless they have clear, justifiable and documented reasons for doing so; otherwise, data held by the organization and any relevant third parties should be destroyed."*

Why get rid of data?

Retaining data longer than necessary increases the risk that information is leaked or accessed by "adversaries" (i.e., people whom you do not want to access your data). Additionally, as time goes by and staff inevitably change, it becomes more difficult to ensure that data is accurate, that new staff are aware of the limitations set on a certain data set and that a data source can be accurately traced.

An organization holding data is responsible for the data it holds – particularly program participant data. As such, it must be able to respond to requests from participants to access their personal data. The more data an organization holds, the more difficult this becomes, both in terms of the time required to answer a larger numbers of requests, and the technical aspects of finding and isolating the relevant data. As a leading privacy expert warns: “If you have information, someone will demand you give it to them.”

...but not too soon!

Discarding data too soon can also be harmful to programming. It is possible to discard data that partners or other stakeholders may need, and it can be very difficult or impossible to retrieve discarded data (if you have deleted it properly!). Depending upon your program type and funding structure, you may need to retain relevant data to justify decision-making and to refer back to for monitoring, evaluation and learning purposes.

WHAT HUMANITARIANS CAN DO:

Create a **Retention, Archival** and **Disposal (RAD) plan**

A RAD plan is a systemic way to manage program data. RAD plans can be customized for different situations. (See sample RAD plans links in the Additional Resources section at the end of this tip sheet.) In general, all RAD plans should describe:

- The **types of data** the organization must retain (and why)
- The **length of time** the data should be stored (and why)
- The **format** in which such data should be stored (and why)
- **How** the data will be retained, archived, transferred and destroyed
- **Who** is authorized to delete data (referred to as a “RAD Officer”), and who is responsible for confirming all organization data is properly destroyed before disposing of organization equipment. (Assigning these responsibilities to a job function (e.g., the M&E or IT officer) rather than a named team member can help ensure continuity of coverage if there are staff changes.)
- **Who** is covered by the plan and team member roles/responsibilities
- The **penalties** resulting from plan violations

All staff with a responsibilities related to this plan should sign that they understand the plan and pledge to uphold its tenets. Plans should also clearly state that no organization officer, employee or other representative is to modify, delete or destroy any data in violation of local, state, national, international or industry regulation.

Create an information inventory

A single program may contain various data sets and different approaches to gathering this data. The first step in managing data is to map out exactly what information is held, where it is held, and what the retention needs are for each type of data.

To do this, organizations often create an “information inventory” in conjunction with their RAD plan. An information inventory is a document that identifies steps within a program where major information groups are collected, and provides a complete list of the locations where they are held (e.g., on a certain computer, USB, hardcopy with the finance/program/M&E team in a field office or country head office, etc.).

Understand your legal environment

Different data retention laws apply depending upon the country/countries in which you work. Cross-border programs may face even more complicated regulations. If you are unsure which data retention laws apply to you – or are gathering particularly sensitive data – you may want to seek legal counsel to ensure you interpret and apply data retention laws appropriately.

Ensure good tagging and data provenance

Make sure the data you archive is understandable to someone unfamiliar with your program. This can mean labeling your files well, tagging information with labels that are clear to outsiders and/or leaving an inventory of the folders you have archived with a clear description of the folder structure.

Recording **data provenance** is the process of documenting data's origin and the path it took to end up in its current state (e.g., labeling how and when it was collected and how it has since been edited). Make sure to tag or label your data so someone can clearly tell where it came from, when it was collected, and how it was collected so that it can effectively be used in the future. As an example, when saving survey data, include the questions that were asked alongside it.

Be clear about what is shared with whom

Depending on your organization's policies, some staff may share files from personal accounts, rather than work ones. When these team members leave, their work accounts are disabled, but access to organizational files from their personal accounts often remains open. Wherever possible, keep work-related data on work-related accounts and encourage your team to do the same. If boundaries between work and personal accounts have already blurred, regularly verify who has access to what data and adjust sharing permissions accordingly. This might mean periodically removing access for personal email addresses that can log in to organization platforms or updating the authorized users of software tools each time new staff are hired.

Include a backup in your retention and archiving plans

If it is especially important to retain and archive certain data (e.g., in the event of a donor audit), make sure a backup of this data exists. Store critical data on a second hard drive in a different location or a second online location in the event the first version is lost or damaged. If you are storing a backup of PII, make sure that both the original version and the backup version are held with the same security and protection measures in place. Also, when it comes time to dispose of PII data in one location, the same procedure or actions are applied to the backup PII. Make sure the backup locations are clear (by listing in your information inventory, for example) so newcomers can keep track of critical data and the backup.

Plan for data usability

When deciding upon a format in which to save data, consider the length of time you will be saving it. Will someone with different software or operating systems still be able to open your data? As "dead formats" become more of a reality, make sure to save your data in common formats rather than "unusual" ones. The same principle applies to which cloud-based company you may choose; think how likely it is that the company will be in existence in a few years' time and opt for more established services, or open source options, rather than a new start-up, for long-term storage.

Clearly communicate your archival plan

If you will archive certain data, consider the length of time you will need to keep it and give clear instructions to anyone who may follow you. This might mean including a 'README' document along with the data on whatever storage device you choose, which states clearly when the data should be disposed of and how. Alternatively, make sure that a document (and maybe a calendar alert as well) with these instructions is evident to team members who may join after you (or others) have left.

Clearly communicate your archival plan

If you will archive certain data, consider the length of time you will need to keep it and give clear instructions to anyone who may follow you. This might mean including a 'README' document along with the data on whatever storage device you choose, which states clearly when the data should be disposed of and how. Alternatively, make sure that a document (and maybe a calendar alert as well), with these instructions is evident to team members who may join

after you (or others) have left.

Use secure data disposal tools

As the digital security guide *Security in a Box* states, “From a purely technical perspective, there is no such thing as a delete function on your computer.” So, while you might think that emptying the “Recycle Bin” on your computer is sufficient, that document has not been deleted securely. When you are certain that you want to dispose of data, make sure you do so effectively. Refer to the open source tool *Eraser* and Security in a Box’s *“Destroy Sensitive Information”* post for specific guidance.

ADDITIONAL RESOURCES:

10 things you should know about long-term data archiving. TechRepublic. July 2010.

Creating the records retention schedule you need. TAB. December 2012.

Deleting Personal Data. UK Information Commissioner’s Office (ICO). An explanation of what is meant by “archiving”, “deleting”, “destruction” and “beyond use”.

The importance of data retention policies. TechRepublic. July 2006.

Retaining Personal Data. UK Information Commissioner’s Office (ICO). Principle 5 of the Data Protection principles: “you to retain personal data no longer than is necessary for the purpose you obtained it for.” This is part of a useful data protection guide for organizations, but focuses on *personal* data.

Security in a Box: Destroy Sensitive Information. Frontline Defenders and Tactical Technology Collective. A how-to on destroying sensitive information.

Training curriculum on data retention and backup, with a focus on digital security. LevelUp.

Examples of RAD policies

- Central Kentucky Riding for Hope, INC *record retention and destruction policy.*
- Sheffield Health and Social Care *retention and disposal policy* (includes an implementation plan).

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

GLOSSARY OF TERMS

TERM	MEANING
Archiving	Archiving is a general term for the range of practices and decisions that support the long-term preservation, use, and accessibility of content with enduring value; intentionally preserving data in a way that makes it easy for collaborators to refer back to it. *(Responsible Data Forum)*
Biometrics	Biometrics refers to the measurement of unique and distinctive physical, biological and behavioural characteristics used to confirm the identity of individuals *(Privacy International)*. Examples include fingerprints, iris scans and voice recognition.
Cloud Hosting	Cloud Hosting refers to the on-demand delivery of IT resources and applications via the Internet with pay-as-you-go pricing. Cloud Hosting provides a simple way to access servers, storage, databases and a broad set of application services over the Internet. *(Amazon Web Services)*
Data Controller	The agency or person who determines the purposes for which and the manner in which any personal data are, or are to be, processed. *(CaLP)*
Data Processor	The affiliate/ service provider; a person who processes personal data on behalf of the data controller over the course of rendering the services. *(CaLP)*
Data Provenance	Data provenance refers to the source and history of a data set, including how it was collected and manipulated.
Data Subject	A living individual who is the subject of the personal data, i.e. to whom the date relates either directly or indirectly.
De-identification	The a process of taking identifying information that can connect data with an individual out of a data set. *(Responsible Data Forum)*
Data Disposal	Deleting data in a safe and responsible way; organisations should not hold beneficiary data for longer than is required unless they have clear, justifiable and documented reasons for doing so. *(CaLP)*
Data Disposal	Any electronic substitute for cash that provides full flexibility for purchases. It may be stored, spent, and/or received through a mobile phone, prepaid debit/ ATM card or other electronic transfer. *(ELAN)*

TERM	MEANING
Data Retention	The length of time that data is kept by the organization that gathered it.
Encryption	Encryption is a way to protect sensitive information by scrambling it, so that it is unreadable by anyone without the specific decryption method required. It is possible to encrypt an email, specific files, or the content on an entire computer.
End to End Encryption (E2EE)	End to end encryption (E2EE) systems are digital systems that facilitate secure, encrypted communication over untrusted networks.
E-Transfer	A digital transfer of money or vouchers from the implementing agency to a program participant. E-transfers provide access to cash, goods and/or services through mobile devices, electronic vouchers, or cards (e.g., prepaid, ATM, credit or debit cards). *(ELAN)*
E-voucher	A card or code that is electronically redeemed at a participating distribution point. E-vouchers can represent cash or commodity value and are redeemed using a range of electronic devices. *(ELAN)*
Financial service provider (FSP)	An entity that provides financial services, which may include e-transfer services. Depending upon your context, financial service providers may include e-voucher companies, financial institutions (such as banks and microfinance institutions) or mobile network operators (MNOs). Financial service providers include many entities (such as investment funds, insurance companies, accountancy firms) beyond those that offer humanitarian e-transfers. *(ELAN)*
Know Your Customer (KYC)* *Note: KYC is also known as Customer Due Diligence	'Know Your Customer' refers to the information that the local regulator requires banks to collect about any potential new customer in order to discourage financial products being used for money laundering or other crimes. *(CaLP)*
Personally Identifiable Information (PII)	Any data that directly or indirectly identifies or can be used to identify a living individual. (Examples include names, phone numbers, bank record details, and biometric data such as fingerprints or iris scanning) Note that PII can be also be any combination of data sets (sometimes seemingly innocuous ones) that would *allow for individual identification.*
Privacy Impact Assessment (PIA)	A Privacy Impact Assessment (PIA) is a tool to analyze and mitigate the potential privacy risks to individuals as well as privacy and data protection compliance liabilities for the organization for any program or activity.
Privacy Impact Assessment (PIA)	A Privacy Impact Assessment (PIA) is a tool to analyze and mitigate the potential privacy risks to individuals as well as privacy and data protection compliance liabilities for the organization for any program or activity.

TERM	MEANING
Short Message Service (SMS)	Short Message Service (SMS) commonly known as ‘text messages’, SMS is a way to send short messages using an alphabet, numbers, and symbols. SMS messages are digital information that can be transmitted over mobile networks, without Internet signal. *(FrontlineSMS)*
Secure Sockets Layer (SSL)	Secure Sockets Layer (SSL) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers. *(ssl.com)*
Sensitive Personal Data	Sensitive personal data is a particular category of personal data, relating to the following: • Racial or ethnic origin, • Political opinions, • Religious, ideological or philosophical beliefs, • Trade Union membership, • Information relating to mental or physical health, • Information in relation to one’s sexual orientation, • Information in relation to commission of a crime and information relating to conviction for a criminal offence *(Innovation Value Institute)*
Standard Operating Procedures (SOPs)	Standard operating procedures (SOPs) are written instructions intended to document how to perform a routine activity. Many companies and organizations rely on standard operating procedures to help ensure consistency and quality in their products. Standard operating procedures are also useful tools to communicate important corporate policies, government regulations, and best practices.
Two Factor Authentication (2FA)	Two factor authentication (2FA), also known as two step verification, is an account security layer that requires a user to provide a password (something they know) and an additional code (something they have), such as an SMS code sent to a phone or a token.
Unique Identifier (UID)	A unique identifier (UID) is a numeric or alphanumeric code that is unique to an entity within a given system. (e.g., a national ID number for an individual)
Voice over Internet Protocol (VOIP)	Voice over Internet Protocol (VoIP) is a technology that allows people to make voice calls using a broadband Internet connection instead of a regular (or analog) phone line. *(Federal Communications Commission)*

This resource was created by the Electronic Cash Transfer Learning Action Network (ELAN). The ELAN works to improve how electronic cash and electronic vouchers are used to assist survivors of natural disasters and conflict. It brings together staff from humanitarian organizations and the private sector to improve e-transfer programs.

elan
The Electronic Cash Transfer
Learning Action Network

The Electronic Cash Transfer Learning Action Network, convened by Mercy Corps and with support from the Mastercard Center for Inclusive Growth and PayPal, is connecting businesses and humanitarians to improve e-transfers in emergencies.

MERCY CORPS

mastercard. Mastercard Center for Inclusive Growth

PayPal