TIP SHEET 6
RESPONSIBLY SHARING DATA

elan
The Electronic Cash Transfer Learning Action Network

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.

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

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)*****.**

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

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