DATA MANAGEMENT AND PROTECTION STARTER KIT

TIP SHEET 5
ENCRYPTION

elan
The Electronic Cash Transfer Learning Action Network

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 The Responsible Data Forum's. 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.

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