OCHA centre for humdata

THE CENTRE FOR HUMANITARIAN DATA

GUIDANCE NOTE SERIES
DATA RESPONSIBILITY IN HUMANITARIAN ACTION

GUIDANCE NOTE ON DATA SECURITY IN OPERATIONAL DATA MANAGEMENT

KEY TAKEAWAYS:

- Data security is a key component of data responsibility – the safe, ethical and effective management of data for humanitarian response.
- Two common threats to data security in humanitarian action are digital surveillance and interception, and unauthorized or malicious activity.
- Humanitarian actors face many challenges related to data security, including device and application vulnerabilities, poorly secured networks, metadata exposure, physical vulnerabilities, staff capacity and error, and managing sensitive data.
- A lack of robust data security undermines the ability to deliver assistance and protection to affected people, maintain duty of care for staff, and operate effectively in complex environments.
- Data security requires both individual action and broader organizational engagement and investment. This includes adopting relevant policies, guidelines and risk-related mitigation procedures, investing in responsible data management, and promoting actions for data responsibility among staff and partners.

INTRODUCTION

Data security is a key component of data responsibility – the safe, ethical and effective management of data for humanitarian response. It entails a set of physical, technological and procedural measures that safeguard the confidentiality, integrity and availability of data, and prevent its accidental or intentional, unlawful or otherwise unauthorized loss, destruction, alteration, acquisition or disclosure.[1]

Digital technologies such as mobile apps, web-based platforms, and biometric registration systems can improve humanitarian action, but they can also increase the risk of data interception, tracking and unauthorized access. Critical incidents such as the cyberattack on ICRC servers containing data related to the Red Cross and Red Crescent Movement's Restoring Family Links services[2] have shown that the humanitarian sector needs to prepare for and respond to major data security breaches and related threats.

A lack of robust data security undermines the ability to deliver assistance and protection to affected people, maintain duty of care for staff, and operate responsibly in complex humanitarian environments. Humanitarian organizations and staff must understand vulnerabilities related to data security and implement appropriate actions to mitigate risk. This is particularly important in conflict environments.

[1] IASC, 2021. **Operational Guidance on Data Responsibility in Humanitarian Action**.

[2] ICRC, 2022. **ICRC cyber-attack: Sharing our analysis**.

This Guidance Note presents common threats to data security and vulnerabilities in operational data management, and offers a set of recommended actions to improve data security in humanitarian settings.[3]

COMMON THREATS TO DATA SECURITY

Two common threats to data security in humanitarian action are digital surveillance and interception, and unauthorized or malicious activity.

- **Digital surveillance and interception:** Targeted surveillance, often enabled by telecommunications service providers subject to interception requests, may allow state law enforcement and security agencies to access/intercept communications. State and non-State actors alike may also deploy covert surveillance tools, such as masquerading as legitimate cell phone towers known as 'IMSI-catchers', to support eavesdropping on mobile phone communications. Beyond targeted surveillance, many social media platforms collect information on their users, and this data is vulnerable to the same level of exploitation as any other data. Users often have little to no say in accepting updates to the data processing policies, and are often unaware of what data is being generated and processed by the platforms they use or who has access to their data. The abundance of information that can be obtained, inferred or derived from social media data has become increasingly popular with both private and public parties for surveillance and other non-humanitarian objectives.[4]

- **Unauthorized or malicious activity:** Phishing attacks that convince individuals to click a link in communications that appear to come from trusted sources can enable remote access to a device or compromise its contents. Malware may be installed on a device remotely or from compromised links sent through messaging applications, emails and attachments. Less technical approaches, such as theft or impersonation via social engineering, also pose a serious threat to individuals and organizations.

The vulnerabilities described below increase the likelihood of these threats.

COMMON VULNERABILITIES IN OPERATIONAL DATA MANAGEMENT

While data management varies by context and organization, there are several common vulnerabilities faced by humanitarian actors. Humanitarians should assess and reduce these vulnerabilities to minimize the exposure of affected people and staff to threats and potential harm.

1. Device and application vulnerabilities

Using tools or software not approved or vetted by your organization carries a range of risks related to data security. Similarly, outdated or poorly configured software can be exploited for surveillance purposes by allowing attackers to gain control of a device through inadequate security controls.

In addition, mobile devices often have a number of applications that enable surveillance by supporting activity and content tracking, and transmitting geolocation and other metadata to third parties. This applies particularly to free applications, which are often predicated on a business model that exploits personal data.[5] The default settings of applications may also contain inherent vulnerabilities such as defaulting message encryption to off, defaulting cloud back-ups to on or the use of conference recording functionality, which result in conversations being stored on third-party servers.

[3] Operational data management entails the collection or receipt, storage, processing, analysis, sharing, use, and retention and destruction of data and information by humanitarian actors. IASC, 2021. **Operational Guidance on Data Responsibility in Humanitarian Action**.

[4] Privacy International and ICRC, 2018. **The Humanitarian Metadata Problem - Doing No Harm in the Digital Era**.

[5] Privacy International, 2020. **Privacy shouldn't be a luxury**; also Privacy International, 2019. **Buying a smartphone on the cheap? Privacy might be the price you have to pay**.

2. Poorly secured networks

Using public or open Wi-Fi networks (i.e., those without a password) may expose humanitarians to surveillance and may also lead to intrusion, such as unauthorized parties joining group chats or online meetings. This vulnerability can also arise when an organization has not properly configured its own servers, routers and services. The default settings are often overly permissive and may allow attackers to gain access to devices and networks. The aim of this type of intrusion can be to identify and profile devices and users of a network, their geographic location, the people they have communicated with, and even the content of the communication.

3. Metadata exposure

All digital activities leave digital footprints, often referred to as metadata, on devices, servers and network infrastructure. Metadata describes information about the data in question. For example, when sending an email, the metadata would include the time sent and the IP addresses of recipient and sender. Humanitarian organizations passively generate metadata through internal communications, exchanges with people affected by crises, and during programme implementation and monitoring.[6] Access to such metadata can be as intrusive and revealing as access to any other data. It can reveal information about individuals such as their location and recent activities which can enable re-identification and targeting by malicious actors.

4. Physical vulnerabilities

There are a number of physical vulnerabilities that might lead to unauthorized access to data and information by malicious actors. For example, staff might encounter checkpoints at which they are required to hand over devices and documents. There is also a risk of physical surveillance: anyone within the vicinity of a meeting with an interlocutor could overhear discussions or deliberately listen-in to the conversation. Finally, devices are at greater risk of being lost or stolen when they are taken out of secured office environments.

5. Staff capacity and error

Poor practices and inconsistent application of data security measures can exacerbate existing vulnerabilities or create new ones. Staff might be unaware of the vulnerabilities related to data security and how to mitigate the associated risks. Resource and time constraints might also have negative effects on how staff handle data when prioritizing other areas of work. For example, staff may share sensitive data without encrypting the file (i.e., requiring a password to open it) thereby increasing the risk of inadvertently exposing the data.

6. Managing sensitive data

Sensitive data, such as data from household surveys, needs assessments and other forms of microdata, makes up an increasingly significant volume of data in the humanitarian sector. While this type of data is critical to humanitarian action, it can cause significant harm to individuals or organizations if accessed without proper authorization. Managing sensitive data exacerbates other vulnerabilities by increasing the severity of potential harm. It can also increase the likelihood of targeted attacks, including interception and unauthorized access.[7]

[6] Privacy International and ICRC, 2018. **The Humanitarian Metadata Problem - Doing No Harm in the Digital Era**.

[7] Both personal and non-personal data can be sensitive. For more information, see IASC, 2021. **Operational Guidance on Data Responsibility in Humanitarian Action**.

RECOMMENDED ACTIONS FOR DATA SECURITY

Humanitarians should take the following actions to improve data security in their work.

Understand the risks in your environment

- Identify and assess risks by conducting a Data Impact Assessment (DIA).[8] DIAs provide an understanding of the potential consequences of a data management activity.
- Redesign or cancel an activity if the foreseeable risks of data management outweigh the intended benefits.
- Regularly consult relevant news, briefings and security reports to inform the understanding of risks in your environment.
- Adapt your approach and choices to the situation. A tool or technology might be appropriate in one context, but unsuitable in another.

Practice good password management

- Secure your devices and accounts with strong passwords that include numbers, capital and lowercase letters, and symbols with at least 16+ characters per password.
- Enable multi-factor authentication (MFA) for all accounts.
- Do not reuse the same password for multiple accounts and update passwords regularly (unless MFA is being used).
- Do not store your passwords physically (on notes) or digitally (in a file on your device) and do not share your password with others.
- Do not enable the 'Remember Me' functionality in applications and browsers.
- Use a password manager, preferably one recommended, approved or managed by your organization.
- Use a password leak monitoring service to regularly check whether your password has been compromised.
- Change your passwords on all accounts immediately if your device is lost or stolen.
- Use incognito or private browser tabs as often as possible.

Use antivirus/anti-malware software

- Make sure that you have appropriate antivirus/anti-malware software on all devices.
- Always check with an IT specialist in your office if available or otherwise with colleagues at a partner organization to select the right tool and configure it appropriately.

[8] See the **Guidance Note on Data Impact Assessment** for additional information on how to conduct a DIA.

Keep software and operating systems up to date

- Check regularly that your device, software, applications, and browser plug-ins are up to date and enable automatic updates for your operating system.
- Use web browsers that receive automatic security updates.
- Avoid the use of software for which future maintenance is likely not to be available.
- Shut down devices regularly or when prompted by your system to enable updating and protect against attacks.

Avoid phishing scams and be careful what you click

- When receiving suspicious emails or other messages, always check the sender's address/contact information and only click on links or attachments from trusted senders.
- Even if the link is from a trusted sender, always copy it and use a private or incognito browser tab to open it.
- Always check that the URL corresponds to a known, reputable website by running it through a search engine to ensure the website is legitimate.
- Hover over a URL link before clicking it to see where the link is actually taking you.
- Do not reply to suspicious emails or forward them to your colleagues.
- Report any suspicious activity through the appropriate channel within your organization.

Use mobile devices responsibly

- Use separate devices for work purposes wherever possible. Keep your work devices in a secure place at all times and avoid carrying them around unnecessarily.
- Use messaging tools approved by your organization that provide end-to-end encryption.
- Minimize the use of Bluetooth connectivity and location services, and turn them off when possible.
- Use a Virtual Private Network (VPN) when working online. Consult the IT department or your colleagues for a list of approved tools.
- Always sign out of your account(s) if you are using a public/shared computer or device.
- Do not access sensitive services or information on public/shared devices unless absolutely necessary.
- Disable biometric unlock features—particularly when in transit.
- Verify that your device does not track activity or content and disable those functions where possible.

Practice data minimization

- Only collect the minimum amount of data required to achieve the objective and purposes for a given data management activity.
- Only retain sensitive data when strictly necessary and for as long as necessary to fulfill the purpose for which it is being managed and as required by applicable guidance, law and regulations.

Safeguard sensitive data

- Transfer and store data using approved tools and channels (locally on an internal server, computer or laptop, or on servers and systems operated by your organization, using end-to-end encryption).
- Password protect and/or encrypt files (Word, Excel, PDF) containing sensitive data and share document passwords through separate channels (i.e., text a password for an emailed document).
- Limit and carefully monitor the number of people with access to sensitive data.
- Define a retention and destruction schedule for all data managed by your organization and use appropriate tools for the destruction of data.
- Do not discuss sensitive information in public settings and ensure that no unauthorized persons have access to your meeting spaces, both physical and online.
- Encrypt your email messages.
- Maintain a Data Asset Registry[9] that indicates the level of sensitivity for each data type managed by your office. Review sensitivity levels regularly as the context evolves.
- Consider developing a Data and Information Sensitivity Classification for your context, either as part of an Information Sharing Protocol[10] or as a standalone document for reference.[11]

Organizational investment in data security

Beyond the individual actions outlined above, data security requires broad, organization-level engagement. Organizations need to invest in data security measures to promote data responsibility across their offices and teams. This might include adopting relevant policies and guidelines, risk-related mitigation procedures, investing human and financial resources in data security and management, and promoting data responsibility among staff and partners.

COLLABORATORS: **PRIVACY INTERNATIONAL**; **YALE UNIVERSITY, JACKSON INSTITUTE OF GLOBAL AFFAIRS**.

The **Centre for Humanitarian Data** ('the Centre'), together with key partners, is publishing a series of guidance notes and tip sheets on Data Responsibility in Humanitarian Action over the course of 2022 and 2023. The guidance note series continues work initiated in 2019 and 2020. It also complements the **Inter-Agency Standing Committee Operational Guidance on Data Responsibility in Humanitarian Action** and the **OCHA Data Responsibility Guidelines**, which were published in February 2021 and October 2021 respectively. Through the series, the Centre aims to provide additional guidance on specific issues, processes and tools for data responsibility in practice. The guidance notes and tip sheets published in 2022-2023 have been made possible with the support of the Government of Switzerland.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Foreign Affairs FDFA

[9] The IASC Data Asset Registry template is available **here**.

[10] The IASC Information Sharing Protocol template is available **here**.

[11] See for example the **Data and Information Sensitivity Classification for Ukraine**.