

Information Sharing Protocol (ISP)
Early recovery cluster
Myanmar Earthquake Response 2025

1. Introduction

This ISP supports **data responsibility** in humanitarian action by outlining a common framework, standards, roles, and responsibilities for sharing operational data ethically, safely, and effectively. It applies to **all humanitarian actors** operating in coordinated response settings and aligns with the IASC Operational Guidance on Data Responsibility in Humanitarian Action (2023).

2. Purpose and Objectives

- Strengthen inter-agency coordination and data sharing across the humanitarian system
- Protect affected populations by applying privacy, dignity, and protection standards
- Enable joint analysis and avoid data collection duplication
- Promote safe and ethical handling of sensitive data across all coordination structures

3. Application and Scope

This protocol applies to all operational data management activities including:

- Needs assessments
- Population registration and tracking
- Protection monitoring
- Response tracking, reporting, and analysis
- Case management and vulnerability mapping

4. Data Sensitivity Levels and Examples of Data Types:

The Data Sensitivity levels, and Information Sharing Protocol outlines how different types of data should be handled based on their sensitivity level. Here's a detailed explanation:

Sensitivity Level	Examples of Data Types	Sharing Protocol
Low/Public	HRP, PiN, admin boundaries	Share openly (e.g., HDX, MIMU)
Moderate/Restricted	Assessment datasets, sector beneficiary numbers, 4Ws	Internal or inter-cluster lists
High/Confidential	Community-level assistance figures, partner lists	Inter-agency, limited distribution
Severe/Strictly Confidential	PII (names, age, sex, IDs), GPS of warehouses or facilities	Bilateral, case-by-case via data sharing agreements

5. Data Sharing with Third Parties

Data sharing is permitted only when it serves a **legitimate, proportionate, and necessary purpose** aligned with humanitarian objectives.

- Only based on formal, written requests and consent by the data provider
- Must meet criteria of **specificity, purpose, necessity, and proportionality**
- Include safeguards such as anonymization, retention limits, and confidentiality clauses
- Sharing with third parties must not compromise the **neutrality, independence, and protection** of beneficiaries

6. Data Sharing Agreements (DSAs)

Strictly confidential or personal data can only be shared with a **formal DSA** in place, addressing:

- Purpose and scope of data use

- Security, retention, and access control measures
- Roles and responsibilities of both parties
- Data handling during and post-use
- Alignment with institutional data protection frameworks

7. Actions to Ensure Data Responsibility

- Disseminate the ISP through orientation sessions
- Monitor compliance via the Inter-Cluster Coordination Group (ICCG) or designated Information Management Working Group (IMWG)
- Review the ISP annually or as needed
- Ensure all actors are trained in basic data protection and risk mitigation standards

8. Breach and Dispute Resolution

Any breach should first be addressed bilaterally. If unresolved, it is escalated to the IMWG or ICCG for review. Final decisions rest with the Humanitarian Country Team.

9. ER Cluster Confidentiality Protocol

To ensure transparency, data protection, and respect for partner preferences, the following provisions are established:

- **Opt-out Notification:**
Partners who wish **not to be named or the implementing partner's name** in any external communications—such as reports, visibility materials, or submissions to OCHA—are kindly invited to notify the **ER Cluster Coordinator** in writing via email and CCed to **IMO**. We will ensure your preference is officially recorded.
- **Information Sharing Requirement:**
Regardless of visibility preferences, all partners agree to share a **complete set of activity data including their organization Name** using the standard 4W/5W matrix with the Cluster Coordinator/IMO. This information is essential for effective coordination, accountability to affected populations, and evidence-based planning.

- **Data Anonymization Commitment:**

For all partners who submit an opt-out notification, the **Cluster IMO commits to automatically anonymizing** their identity in any external communication or reporting. This includes removing names, logos, or any identifying references from published documents or shared datasets. No external disclosure will occur without explicit, renewed written consent.