PIM Protection Information Management
For Quality Protection Outcomes

Principles of Protection Information Management[1]

Based on the agreed Protection Information Management (PIM) definition, participants debated at length to further develop the following core guiding principles when engaging on PIM – principles that build on previous inter-agency forums and discussions. These principles underlie and characterize all PIM systems, regardless of their purposes, methods, or products[2].

- **People-centered and inclusive:** Data and information activities must be guided by the interests, well-being, and rights of the affected population and their hosts, which must participate and be included in all relevant phases. Activities must be sensitive to age, gender, and other issues of diversity.

- **Do no harm:** Data and information activities must include a risk assessment and take steps, if necessary, to mitigate identified risks. The risk assessment must look at negative consequences that may result from data collection and subsequent actions or service delivery for as long as the data and information activity is carried out.

- **Defined purpose:** Given the sensitive and often personal nature of protection information, data and information activities must serve specific information needs and purposes. The purpose must be clearly defined and communicated; proportional to both the identified risk and costs vis-à-vis the expected response; and aimed at action for protection outcomes, including the sharing and coordination of protection data and information.

- **Informed consent and confidentiality:** Personal information may be collected only after informed consent has been provided by the individual in question, and that individual must be aware of the purpose of the collection. Further, confidentiality must be clearly explained to the individual before the information may be collected.

- **Data responsibility, protection, and security:** Data responsibility goes beyond data privacy and data protection. It entails a set of principles, purposes[3], and processes that seek to guide humanitarian work and leverage data to improve affected populations and their hosts' lives in a responsible manner while adhering to international standards of data protection and data security. Data and information activities must adhere to international law and standards[4] of data protection and data security. Persons of concern have a right to have their data protected according to international data protection standards.

- **Competency and capacity:** Actors engaging in data and information activities are accountable for ensuring that data and information activities are carried out by information management and protection staff who have been equipped with data and information core competencies and have been trained appropriately.

- **Impartiality:** All steps of the data and information cycle must be undertaken in an objective, impartial, and transparent manner while identifying and minimizing bias.

- **Coordination and collaboration:** All actors implementing data and information activities must adhere to the principles noted above and promote the broadest collaboration and coordination of data and information internally between humanitarian actors and externally, with and among other stakeholders. To the extent possible, data and information activities must avoid the duplication of other data and information activities and instead build upon existing efforts and mechanisms.

---

[1] Developed by the participants at the First PIM Working Meeting held in Copenhagen on 26- 29 May, 2015. The PIM principles take into consideration the 'Principles of Humanitarian Information Management and Exchange', endorsed by the Global Symposium +5 in Geneva (2007) and the International Committee of the Red Cross's 'Professional Standards for Protection Work, Managing Sensitive Protection Data', Chapter 6 (2013).

[2] For how to operationalize these principles, go to the PIM Website at: PIM.guide.

[3] Based in part on the work of OCHA's '*Building Data Responsibility into Humanitarian Action, OCHA Policy and Studies Series*, May 2016; p. 4.

[4] Including the 1990 United Nations General Assembly's 'Guidelines for the Regulation of Computerized Personal Data Files'.