

Principles of Protection Information Management¹

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.² **These principles underlie and characterize all PIM systems, regardless of their purposes, methods, or products³.**

- **People-centred and inclusive:** PIM activities will be guided by the interests and well-being of the population, which must participate and be included in all relevant phases of PIM. PIM activities must be sensitive to age, gender, and other issues of diversity.
- **Do no harm:** PIM 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 as long as the PIM activity is being carried out.
- **Defined purpose:** Given the sensitive and often personal nature of protection information, PIM must serve specific information needs and purposes. The purpose must be clearly defined, communicated, be proportional to both the identified risk and costs vis-à-vis the expected response, and be 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 protection and security:** PIM activities must adhere to international law and standards of data protection and data security.⁴ Persons of concern have a right to have their data protected according to international data protection standards.
- **Competency and capacity:** Actors engaging in PIM activities are accountable for ensuring that PIM activities are carried out by information management and protection staff who have been equipped with PIM core competencies and have been trained appropriately.
- **Impartiality:** All steps of the PIM cycle must be undertaken in an objective, impartial, and transparent manner while identifying and minimizing bias.
- **Coordination and collaboration:** All actors implementing PIM activities must adhere to the principles noted above and promote the broadest collaboration and coordination of data and information internally – both between humanitarian actors and externally – with and among other stakeholders. To the extent possible, PIM activities must avoid the duplication of other PIM efforts and instead build upon existing efforts and mechanisms.

¹ Principles of Protection Information Management, as developed and agreed by PIM Stakeholders, in the first PIM Working Meeting, May 2015

² 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)

³ For how to operationalize these principles, go to the PIM Website at: PIM.guide

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