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.[2] These principles underlie and characterize all PIM systems, regardless of their purposes, methods, or products[3].

- **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'

Defined purpose: Given the sensitive and personal nature of protection information, PIM must serve specific information needs and purposes. The purpose must be clearly defined, be proportional to both the identified risk and costs vis-à-vis the expected response, and be aimed at action for protection outcomes.

ACCESS INFO LANDSCAPE

- **Define Purpose and Information Needs:**
  - Define the specific protection objectives and activities to be informed by information management system. The purpose of the information management system or activity must aim to enhance the safety and dignity of the persons and/or the population involved; as such it should be used to inform protection activities. The purpose must take into account the information needs of the affected individuals and communities to ensure effective accountability to affected populations.
  - Focus on the purpose and the information needed to meet that purpose, rather than on data. Think broadly about the purpose of the system, so that critical information is not overlooked. It is Important to also know when defining the purpose, what the actual goal is or what you will use the information for.
  - Assess and specify the audience of the data, information and analysis; who will use the information and how it will be used.
  - Distinguish between what is essential (information you need to have and you will be able to use and analyse) versus desirable (information that is nice to have). This prioritization can also examine issues around the relevance of the information needs against the purpose, and the proportionality or balance between concerns regarding the expected risks and benefits of the activity.
  - As the project is implemented and data is collected, new information needs may emerge. The purpose may have to be reviewed accordingly. If the task or information needs change significantly, then a new purpose (and all its associated components) may need to defined and applied.
  - As per data protection principles, information cannot be used for purposes other than for which it was originally collected, and in the case of personal data, for which consent has been received. It should not be used for other purposes without additional consent and a further assessment of the risks associated with the new purpose(s).
  - Protection actors must only collect information on abuses and violations when necessary to enable a protection response. When defining information needs ensure there is the capacity to respond to identified needs, or procedures to refer people appropriately.
  - Define metadata information needs.
  - Bring together a multi-functional team of IMOs and non-IM sector specialists when defining the information needs.
  - Always collect only what data is need, and intend to use all that is collected.

- **Data and Information Review:**
  - A secondary desk review and consultations with relevant partners can help determine if needed information exists, and if and how it can be accessed. The information we need to fulfil the purpose may already be available, or may become available in the near future. A secondary desk review and consultations with relevant partners can help determine if information exists, and if and how it can be accessed.
  - Make use of what has already been collected to avoid duplication of efforts as well as unnecessary burdens on and risks for data subjects.

DECIDE AND DESIGN

- **Information Sharing:**

- Once the purpose is defined, share it with key actors supporting to ensure that the purpose is both well understood and agreed.
- The purpose of the exercise should guide decisions about if and how data will be disseminated, with whom, and at which level of aggregation. Determine the need for an information-sharing network or protocol, what information could be shared, at which level of aggregation, and with which actors, as it relates to agreed purpose of the information system.
- Whether or not information sharing is envisaged, communicate the purpose of the information system to partners and other organizations present. This creates an opportunity for collaboration to achieve complementary purposes, avoids situations where similar purposes are being pursued in parallel efforts, and helps to determine if information sharing would be desirable.
- Every data collection system should have the purpose of sharing some level of data or analysis.

❖ **Design with Affected Population:**

- The insights and knowledge of the affected populations can identify and better understand the needs, threats, vulnerabilities and priorities of individuals, communities and specific groups within those communities; the potential challenges, risks and benefits associated with a proposed PIM purpose and activity; cultural and social sensitivities surrounding the use of certain data collection methodologies or tools; context and security considerations, etc.
- Vet the defined purpose with people concerned to ensure that the purpose is both well understood and agreed. Consult with the affected people to ensure that the purpose is anchored in a ground-level reality. i.e. well understood, appropriate and suited to the circumstances, and more likely meet the needs.
- Discuss the conclusions of the risk assessment with the affected population to ensure that the risks assessment properly reflects the concerns and experiences of the affected population.
- Communicate the purpose widely, clearly and regularly. Make messages available in local languages, tailored to the operational context, and delivered in protection-sensitive methods and channels that are accessible to and understandable by various groups, such as the illiterate, the blind, the deaf, the elderly, children, the marginalized, and other vulnerable groups. Take into consideration insider and outside perspective to ensure the defined purpose has both perspectives - is nuanced and reduces potential bias.

❖ **Design Information System:**

- Ensure modalities of the PIM activity and its associated information systems are guided explicitly and deliberately by the specific purpose of the exercise. I.e. - explain details on who will be targeted for data collection, how and when the information will be collected, and expected challenges in fulfilling the purpose.
- Clearly communicate information on the purpose of the PIM exercise to internal colleagues and partners who will be involved.
- Secure a shared internal understanding of the purpose will help to forestall time-consuming discussions later on about who is targeted for data collection, what methodologies and tools are used, and which information-sharing networks or protocols are in place.
- Work with risk assessment to ensure do no harm is adhered.

IMPLEMENT

❖ **Conduct Data Collection:**

- Prior to data collection, it is important for data collectors and other field staff to have a clear understanding of the specific purpose of the PIM exercise. With clarity of purpose, we can avoid situations in which they might omit valuable information because they do not realize how important it is, or they expose people to harm by collecting sensitive information that will not be used later on. Clarity of purpose enables data collectors to draw the line between what is relevant and what is interesting, i.e., between what is needed for the purpose and what is not. This also gets a specific meaning in qualitative data collection where the

questions and tools are often less strictly structured and much more responsibility in terms of guiding the discussion is on the data collector.

- Data collectors should begin their engagement with data subjects by clearly communicating information on the purpose of the PIM exercise. This is important for a number of reasons:
  - To build trust and promote cooperation from data subjects, notably by dispelling rumors and misconceptions. For example, key informants and local communities may be unwilling to share information due to fears it will be shared with authorities and subsequently used against them. In other cases, people may be willing to share information because they assume that humanitarian assistance will follow, and become hostile and uncooperative if this is not the case. Clearly explaining the purpose at the outset can increase the likelihood that data subjects will share information by assuaging their fears and calibrating their expectations.
  - To create a basis on which data subjects can provide or withhold informed consent.

❖ **Process and Analyse:**

- The scope, tools and level of data analysis should be guided by the specific purpose of the PIM activity. For example, if the purpose is to identify protection risks for internally displaced people to inform effective responses (protection monitoring), descriptive analysis should be conducted to summarize and compare the data to answer the basic who, what, when, where. If the purpose is to explain why certain groups seem to be targeted for specific kinds of attacks, explanatory analysis is better suited.
- Protection principles should also guide the data analysis process, particularly when it involves personal data. Personal data should not be processed in a way incompatible with, irrelevant to, or excessive to the purpose(s) for which it was initially collected.

❖ **Disseminate and Share:**

- Examine evolving needs for certain sets or levels of protection information, which they may need to make decisions for themselves and their families, what's the timeframe for this information
- Ensure data and information is shared in a timely, appropriate, accessible and predictable manner - based on defined purpose and stakeholder analysis, and agreement (reached earlier) with key stakeholders.
- Ensure the risks have been assessed (again) form a 360 degree view to determine if the context or the environment has changed such that the sharing of information could do harm.
- Unless specific consent has been obtained, personal data should not be disclosed or transferred for purposes other than those for which they were originally collected, and for which the consent was given.

❖ **Store and Maintain:**

- The storage and maintenance of data is guided by data protection principles, according to which:
  - The period for which personal data is kept should not exceed that which would enable the achievement of the specified purpose
  - Personal data should be updated when necessary to ensure it fulfils the purpose(s) for which it is processed.

EVALUATE

- Monitor and review the purpose: As the project is implemented and data is collected, new information needs may emerge. If the task or information needs change significantly, a new PIM purpose (and all its associated components) should be defined and applied.

Informed consent: 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.

ACCESS INFO LANDSCAPE

- **Define Information Needs:**
  - Define purposes and specific uses for which personal or sensitive data is needed.
  - All personal data, depending on context, may be considered as sensitive and as such ensure it always treated in a confidential manner.
  - Identify the information that will require informed consent or where confidentiality may be an issue.
  - Verify that any sensitive and personal information is essential to analysis; otherwise do not collect it or do so anonymously.
  - Examples of information that would need informed are personally identifiable data.
- **Data and Information Review:**
  - Do not ask for personally identifiable information from other data sources unless necessary.
  - Ensure confidentiality and informed consent practices are respected in any secondary data review.
  - Obtain sufficient details on informed consent from secondary data source, including purposes for which data was collected and for which consent was obtained, to ensure original informed consent includes the new intended use.
  - Identify limitations with previously collected informed consent with regards to defined purpose.
  - Conduct secondary data review on anonymized data unless individual case interventions are planned.
  - According to protection principles, unless specific consent has been obtained, personal data should not be disclosed or transferred for purposes other than those for which they were originally collected, and for which the consent was given. This applies to a secondary data review as well. Include reference to informed consent

DECIDE AND DESIGN

- **Information Sharing:**
  - Discuss with information sharing partners what purpose they intend for the data, and ensure that these are sufficiently well reflected in the overall purpose when obtaining consent, or when consent was obtained.
  - Discuss with information sharing partners how to minimize collection and sharing of personal data so as to reduce risks of breaches in confidentiality.
  - Discuss and agree with information sharing partners on how breaches in confidentiality will be handled, such as when data is shared without proper consent.
  - Agree on procedures when and response when consent for sharing of data or information is not granted or is refused (for example when one member of a household not does agree to sharing of their information).
  - Data sharing protocols should specify nature and sensitivity of confidential data.
  - Data sharing protocols should specific purpose(s) coherent with those specified when obtaining informed consent.
- **Design with Affected Population:**
  - Explain confidentiality and informed consent in terms understood by the population and with examples relevant to the context.
  - Work with the community to facilitate and develop clear key messages around informed consent and confidentiality specifically related to the purpose of the activity.

- Discuss implications if people choose not participate in data collection, or do not agree to data sharing or a specific purpose foreseen within the consent.
- Explain the planned data sharing arrangements (with whom, for which purpose), such as referrals.
- Work with the community to understand how the choice of a numerator can influence informed consent.

❖ **Design Information System:**

- Design data collection, analysis and storage that ensure that informed consent is being gathered in relation to the specific purpose or purposes.
- Ensure that personal data and sensitive information can be stored in a confidential manner.
- Ensure sufficient time within the data capture process to get informed consent.
- If personal and sensitive data is collected, be sure that confidential data can be collected from data subjects in a secure and safe space, and in a manner that protects confidentiality.
- Test informed consent forms statements with the people concerned prior to data collection.
- Design data collection tools to record if consent has been given, and for which purpose(s).
- Provide relevant information on data storage and retention plans in purpose and consent statements.
- Depending on the data collected and the purpose, determine if consent must be written or verbal. Written consent, while often preferable, is inappropriate if no personally identifiable information is being collected (e.g. do not collect names in written consent forms if names are not being collected as part of the data collection activity).
- Include procedures for obtaining informed consent in standard operating procedures for data collection.
- Establish a mechanism to allow data subjects to assess, modify and withdraw consent before during and after data sharing, alerting data transfer partners when consent is modified by the data subject.

IMPLEMENT

❖ **Conduct Data Collection:**

- Read an informed consent statement to respondents at the start of the interview.
- A parent or guardian must provide consent prior to participation by a child or adolescent.
- When interviewing individual provide respondents with information on:
  - The purpose of the interview/assessment
  - The expected duration of the interview and the procedures
  - The data to be collected including photos, video and recording
  - How the data is intended to be used
  - How the data will be stored and for how long
  - That the participation is voluntary
  - Known risks to the respondent (is this possible or is this a risk?)
  - Potential benefits to the respondent
  - The right to make complaints and to whom
  - That the respondent may refuse to answer any question or terminate participation at any time.
  - Right to confidentiality

❖ **Process and Analyse:**

- Unless necessary for the specific purpose, personal data should be anonymized prior to storage and analysis.
- In case personal data is required for a specific purpose (i.e. direct assistance to the individual), processing shall not be done without the prior explicit description of its purpose and will only be done for that purpose, and after prior informed consent of the individual concerned.
- Remove any data for which consent was not obtained from the analysis, and from data sharing procedures.

❖ **Disseminate and Share:**

- In general, sharing and dissemination should be done in aggregated format or based on anonymized or unidentifiable data.
- Only share Identifiable information for the purposes described in the informed consent, and where informed consent has been obtained.
- Ensure data sharing procedures respect confidentiality of data and information.
- When disseminating or sharing data, share information on consent obtained for which purpose(s).

❖ **Store and Maintain:**

- Only stored personally identifiable information when necessary and when in informed consent has been obtained for that purpose.
- Only store information for as long as required by the intended purpose.
- Establish decommissioning policies and procedures of all data with particular focus on personal and sensitive data.
- Store agreements and refusals for data to be used for a particular purpose so that informed consent can always be respected for as long as data is retained.
- Dispose of data as per informed consent statement.

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.

ACCESS INFO LANDSCAPE

- **Define Purpose and Information Needs:**
  - The information needs should be relevant to the purpose and proportional to the risks of the exercise. Protection actors should only collect information on abuses and violations when necessary for the design or implementation of protection activities.
  - Define sensitive data within the specific operational context; this is the set of information that can be voluntary or involuntarily misused to harm the physical, legal, material, and psychosocial well-being and interest of the data subject. Periodically review the definition.
  - When determining the nature, scope and level of detail of the information needs, assess the potential risks for all parties involved in or affected by the exercise. Reflect on who will be targeted for data collection, and at which level of precision, depth, reliability and accuracy the data has to be collected to achieve the purpose.
  - Balance the need to gather information to inform beneficial action and the potential risk of harm to the people who provide and collect data. Carefully reflect on the acceptable threshold between the expected risks and benefits of the exercise, and the vulnerabilities or suffering that it seeks to prevent or remedy.
  - When assessing risks, be aware that the data collected now for a specific purpose may be used in the future for another purpose, and that the data that is innocuous now may become more sensitive over time, depending on how it is used or how the security and political context evolves. Do not collect the data unless it will be used; doing this will significantly reduce risk of harm.
  - Data on sexual violence should only be collected when services are available; if services are not available, gender and sexual violence information can only be collected once safe context specific modalities have been identified, including proxy indicators and key information's, for the purpose of establishing appropriate services, providing information to actors who are planning to establish appropriate services or informing advocacy efforts.
  - Conduct a do-no-harm analysis to identify risks, opportunities, legal and ethical issues related to data collection, processing, analysis and dissemination. The defined purpose should be assessed against potential risk: risk of collecting, not collecting, risk of sharing, not sharing, risk to people, risks to colleagues, humanitarian response. This should be a 360 view of risk. PoC, risk to staff and colleagues - a 360 view of risk. Explore the need to review ethical and legal issues through an external or independent party or through the use of internal panels or partnerships.
  - Define, discuss and assess as a community the risk of data and information use.
- **Data and Information Review:**
  - Use the secondary desk review (SDR) to identify risks linked to certain types of data categories or data collection methods.
  - Consult partners and other organizations present to take stock of their activities and lessons learned, and to identify opportunities for collaboration and data sharing. This will allow to avoid duplication of data collection efforts as well as unnecessary burdens and risks for data subjects.
  - The SDR and consultations will determine if the information needed is already available, if it is credible and reliable, and if and how it can be accessed. Always collect only what data is need and use everything that has already been collected.

DECIDE AND DESIGN

- **Information Sharing:**

- Information that is shared correctly serves protection purposes, as it disseminates information about needs and threats without exposing sources to repeated questioning or unwelcomed attention. However, people can be helped as well as harmed when data is shared.
- The decision to share information should be based on an analysis of the risks and benefits, legal and ethical considerations, bearing in mind the sensitivity of specific data variables, the privacy and security of individuals, and their informed consent (in the case of personal data). While assessing risks and benefits of data sharing the criteria should be the improvement of the protection environment of individuals and communities assessed.
- Within the framework of informed consent, it is the ethical responsibility of data and information holders to share data and information in a safe and as useful manner with actors who are in a position or have a responsibility to the respond to issues raised.
- Personally identifiable data shall not be collected or shared unless essential to the well-being and protection of the individual concerned, and in consideration for legal and ethical considerations, on the scope of the written consents obtained, and if proportional to the specific purpose for which the data was collected.
- Identify ways to safely share data within the particular context to minimize the negative impact on the individual or the community.
- Consider domestic legal framework on any obligation to share information and data under national law within the risk assessment process, and potential risks domestic legal framework could pose for data subjects.
- Decisions to share or retain individually-identifiable data on minors shall be based on a determination of the best interest of the child.
- Ensure that data is conveniently analyzable and transferable through the elaboration of appropriate meta-data.
- Data-sharing protocols and agreements should be used to formalise data transfers and to ensure protection considerations are systematically assessed. In addition to data protection safeguards and data breach procedures, protocols should describe procedural and technical modalities by which information will be shared; level of aggregation (typological, demographic, location and temporal); specific metadata; and nature of confidentiality and accountability.
- Broader or more informal information-sharing networks can also be created. An assessment should be conducted to evaluate the risks and benefits of involving different stakeholders in the network. For example, local authorities can sometimes help to solve protection issues, but they can also retaliate or punish individuals or communities for having shared certain information. To mitigate such risks, different stakeholders in the network can have access to different levels and types of information. An MOU should also guide the roles, responsibilities and accountabilities of all those involved, as well as safeguards to preserve the privacy, confidentiality and security of personal information in accordance with data protection and collection standards.
- In most cases, personal identifying data should be removed, since we often lose control of how the information is used and with whom it is shared. When data is confidential or sensitive, it can be analysed and shared at the trends level (without personal information) in lieu of the data itself, using methods such as data coding, pseudonymization, and anonymization.

❖ **Design with Affected Population:**

- Affected populations and other people who will be involved or affected by the PIM work can be involved in the design of the work. They can also help planners better identify and understand protection risks, vulnerabilities, threats and coping strategies, as well as feasible and appropriate mitigation measures.
- Affected populations can assist in the stakeholder mapping to identify who will be affected, either directly or indirectly, by the PIM exercise, and what specific harms might occur in the short, medium and longer term. They can also help with scenarios and forecasting, based on their understanding of the local context.

❖ **Design Information System:**

- Revise the information needs or avoid collecting certain types of data if the risk of harm is too high or disproportional to the expected benefits, if mitigation measures cannot be put in place, or if there is not sufficient information to make an informed determination on the level of risk.
- Ensure that meta-data is sufficiently developed to reflect necessarily information to avoid harm, including reporting on the risks associated with use and collection of the data.
- Define accountability of all stakeholders in standard operating procedures.
- Define a clear clearance mechanism of every analysis or data set before sharing them and integrate it in the written guidelines related to the PIM system under implementation.
- Put into place measure to reduce identified and potential risks (anonymised information; coding of organizations and staff name collecting information, not recording sensitive information). When risks encompass benefits or mitigation measures are not possible, do not collect that information; identify potentially sensitive data elements and groups, and asses the risks associated with gathering or hold such data. If there are risks with data collection, consider alternative sources and methods, possible bias, impact of collection frequencies, alternative locations or communication methods, and possibilities of using proxy data. Generally, do not gather data that is especially sensitive.
- Include safeguards to preserve the privacy, confidentiality and security of personal information in accordance with data protection and collection standards should be established as part of this discussion, prior to data collection.
- Put into place safeguards to reduce fraud or identity theft.
- Choose an interview setting allowing confidentiality of interview (i.e. don't interview publically a SGBV survivor because of the social stigma that can be related to such cases).
- Factor in crowd control considerations to the design of your data or information collection system and how to react in case of security/physical threats
- Only collect the data and information which is required for protection programming and response, i.e. data and information which is not available through a secondary data review, is not being collected by partners and which is critical for an informed protection response. Protection actors must only collect information on abuses and violations when necessary for the design or implementation of protection activities. Do not collect the data unless you are sure you will use it.
- Risk/Benefits assessment prior to implementation, potential collection methodologies should be assessed against their expected impact on each category of people involved in the exercise: the collector, the potential sources and their families, and other cooperating persons (e.g., drivers, interpreters, local NGO staff, etc.).
- Certain data elements might pose a risk both to the individual and /or group from whom the information is being collected and the collector. Identify alternative methods or proxy indicators if certain data element is deemed too sensitive or identify mitigation measures. - Measures to reduce threats and vulnerabilities should be included in any implementation guidelines or instructions. Biases that may affect information collection should also be identified and mitigated.
- The roles, responsibilities and accountabilities of all actors involved in the data collection should be clearly identified, as well as protocols for the secure transfer of data from its collection point to its storage and use points (see the principle on ‘Data protection and security’).

IMPLEMENT

❖ **Conduct Data Collection:**

- Assess and inform all concerned staff if the data collection process and the content of the data itself can pose a risk and do harm to the people involved in or affected by the exercise. Continue to assess and monitor risks during data collection.
- Don't force individuals/communities to answer to questions they feel not comfortable with; based on the specific context, pay attention to the presence of individuals observing data collection without participating.
- Pay attention to any sign of fears on individual/communities during data collection.

- Inform individuals that they can refuse to participate in the data collection and do not have to provide any information if they do not wish to. People can stop providing data at any time.
- When collecting personal data, allow people to verify that the information recorded is correct, and allow them to request corrections or deletions.
- Prevention and mitigation measures are especially important during this phase, as it will often involve direct contact between the collector and the source. These measures can include the use of alternative data sources, data variables and indicators, and alternative collection methodologies, collection frequencies, target groups, and locations.
- The collection process should be guided by ethical standards and a code of conduct that is signed and understood by all enumerators. Codes of personal conduct are essential to ensure that no individual action or inaction causes harm, intentionally or unintentionally, or generates additional risks for affected communities and others involved in the exercise. They are also critical in clearly defining the perimeters of acceptable practice, behavior and personal conduct, and emphasize the duty to respect the rights of people who provide information. Amongst others, they have the right to refuse to share information, to access their information, and to report misuse and abuse. When collecting data, enumerators should inform people of the specific purpose(s) for which data will be collected and processed, how their data will be used, whether the data will be shared with other organizations, and other basic facts on the exercise. Respondents have the right to refuse to share information, and should never be coerced.
- The data collection process should be carefully monitored to ensure that both the code of conduct and operating procedures are being respected. Monitoring also allows for remedial measures to be put in place if the exercise is creating protection or security risks. In this regard, the training for data collectors should include written guidelines and practical examples of how to engage respondents and react to protection threats. For example, they should collect data in safe and quiet spaces, bearing in mind privacy, confidentiality and security issues, as well as the sensitivity of the information being gathered. They should also pay attention to signs that respondents are fearful or uncomfortable, or that other individuals are present and observing the data collection. For example, women reporting sexual violence should not be interviewed in public places, where they are both unlikely to be able to share their story and likely to be attacked or stigmatized if their story is overheard. National staff may be particularly vulnerable, as they can be seen as facilitating the gathering of sensitive information for international actors who may or may not be trusted in the community, or scapegoated when assistance does not follow the collection of information.

❖ **Process and Analyse:**

- Like data collection, the data analysis process can put individuals at risk, depending on the type of analysis conducted, the tools used for data processing, the units of measurement, and the level of aggregation.
- Consider if and how the analysis to be conducted could be combined with other past or current analyses in a way that exposes sources to harm, or if the data analysis could be misinterpreted to the detriment of persons of concern. The analysis should always be linked back to and informed by the specific purpose of the PIM exercise.

❖ **Disseminate and Share:**

- Identify and use existing community based information management mechanisms and support those to share feedback or relevant protection information.
- Before it is shared, the data may have to be selected or filtered, and presented in different ways, through different means/channels, or at different levels of aggregation. The need for such adjustments will depend on the recipient and its audience(s), why and how the information will be used, and the likelihood that it will be shared forward with third parties.
- A dissemination strategy should be developed in the planning phase, using a protection lens. The Strategy should start from the premise that personally identifiable data should be shared based on need and protection considerations.
- ‘Do no harm’ promotes a responsible assessment of the different tools and platforms that can be used to disseminate information, and at which level of aggregation. In many cases,

notably when data is confidential and sensitive, information can be disseminated at the trends level to balance the expected benefits of data collection with potential risks.

- **Store and Maintain:**
  - To avoid harm, data has to be safely handled, stored, archived, and disposed of or decommissioned. People involved in or affected by the PIM work may be exposed to physical violence, discrimination, exploitation or other kinds of harm if data is misused, lost, stolen, used without authorization, modified, contaminated, copied or breached. Such considerations should guide the design of information systems that will be used throughout the life cycle of the PIM work, as well as discussions on data transfer, ownership and accountabilities.
  - Ensure contingency plans for the safe destruction or transfer of data in cases of emergency.
  - Data and information need to be safely transferred from the location where it was collected to the end-users, safely handled, safely stored, safely archived, and safely disposed of. For example, sending data via mobile phones that can then be erased could be a safer option than travelling with paper questionnaires, especially when travelling through checkpoints or crossing frontlines. The safety of both paper and electronic records must be ensured.
  - Define ownership of THE RESULT OF ANALYSED data collected and persons having the right to access data archive and ensure organisation/s BEING CUSTODIAN OF THE data set up technical solution to protect the archive (i.e. password).
  - Safeguards to preserve the privacy, confidentiality and security of personal information in accordance with data protection and collection standards should be established also in relation of data storage and archiving; if data is stored on line, assess security of the server hosting data and/or mitigate risks with anonymising individual information.
  - Sensitive data, including personal data in some circumstances, should be deleted when it is no longer needed for the identified purpose.
  - See the principle ‘Data protection and security’ for further details.

EVALUATE

- Carry out a systematic review to identify subsets of a data that were not used for the analysis and for response actions in order to inform future data collection exercises.

Data protection and security: PIM must adhere to international standards of data protection and data security.[1]

ACCESS INFO LANDSCAPE

- **Define Information Needs:**
  - Identify and understand the data protection implications of the data needs of your operations and your partners. Be familiar with the types of personal and sensitive data within your operation and document these in simple and clear language.
  - Identify the organization's data protection policies and guidelines on the collection, analysis and processing of data.
  - Identify the relevant law and legal framework governing data collection and protection within the environment, including data subject legal rights.
  - Identify the data and information which may pose protection risks in relation to the proposed project and define mitigating measures that would be recommended to ensure the protection and security of data, including in case of data breaches or other failures of data protection measures.
  - Verify any sensitive and/or personal information proposed for collection has a defined purpose and the utility of the data outweigh the risks associated with the acquisition of the data. If the data is not essential to decision making and/or programmatic needs, do not collect the data.
  - Document risks associated with data collection, analysis and processing data and information. If appropriate, consider establishing a clearance procedure for the release or use any protection sensitive data to safeguard appropriate sharing and dissemination procedures.
- **Data and Information Review:**
  - Conduct a secondary data review (SDR) to maximize the use of existing data, avoid duplication and minimize any possible risks for both data subjects and their information.
  - Verify if existing data has been collected and processed in accordance with data protection principles. Avoiding using data not collected, processed or used in accordance with fundamental data protection procedures.
  - Any repository of existing data, (secondary data review materials, SDR) should safeguard data, information and sources within the operation/environment. An SDR repository should balance the level of access and security needed to secure safe and ethical storing of all files collected on an ongoing basis.
  - Clarify existing and future data ownership issues, as well as accountabilities for data breaches and misuse.
  - Conduct a risk assessment and correlating analysis, (see Privacy Impact Assessment, (PIA) / Data Protection Impact Assessments, (DPIA) instructions for further details).

DECIDE AND DESIGN

- **Information Sharing:**
  - Verify any existing data and information is regularly available, credible and reliable by consulting with data sources. If yes, work with partners to put in place predictable measures to safely access, transfer and store data on an ongoing basis. Establish data sharing protocols or agreements as is necessary to assist in efficient and ethical sharing over time.

[1] Including for example the 1990 United Nations General Assembly's 'Guidelines for the Regulation of Computerized Personal Data Files', the ICRC 'Professional Standards for Protection Work Carried out by Humanitarian and Human Rights Actors in Armed Conflict and Other Situations of Violence' (2013), the Madrid Resolution on International Standards on the Protection of Personal Data and Privacy (2009), and UNHCR's 'Policy on the Protection of Personal Data of Persons of Concern to UNHCR' (2015).

- Establish data sharing protocols where needed, and take all appropriate technical and organizational measures to protect data, in particular sensitive protection data (including, but not limited to, personal data) against the risk of accidental or unlawful/illegitimate destruction, loss, alteration, and unauthorized disclosure.
- Data sharing protocols should be designed following principle of “Do No Harm”.
- Data sharing protocols should reflect assessed risks to data collectors, and how these risks will be mitigated when data is shared and analysed. Potential risks should be spelled out in the protocol.
- Data sharing protocols should address uses of anonymised data and what and when data is to be shared with the communities.
- Identify the organization's data protection policies, guidelines and/or protocols on information sharing, processing and storage solutions. Check to see if the organization has a code of conduct (or a similar policy) which commits staff to ensure the confidentiality of data, including any mandatory or routine measures of confidentiality.
- Verify any and all information sharing mechanisms have procedures in place to report and respond to potential data breaches (e.g. dispute mechanisms).

❖ **Design with Affected Population:**

- Engage with affected populations to identify what types of data and information might be viewed as sensitive, private, or confidential in a specific cultural, political and security context.
- The protection of individuals is more important that the engagement of the communities.
- Respect the rights of data subjects: the right to access their information, the right to correct and delete data, and the possibility of complaining if data is used in an incorrect way.
- Work with the community to facilitate and develop clear key messages around data protection and confidentiality specifically related to the purpose of the activity.
- Explain the principle of confidentiality, the intended use of the information, how the information will be protected, including sharing arrangements, to people of concern.
- Inform communities of the specific purpose(s) for which data is collected or processed, and whether the data will be transferred or shared with other organizations.

❖ **Design Information System:**

- Determine the most appropriate technical and organizational measures to ensure the safety and security of both physical and soft data files from, (but not limited to), the risk of accidental or unlawful/illegitimate destruction, loss, alteration, copying, misuse, contamination and/or unauthorized disclosure or access.
- Ensure technical and organizational measures are in place to ensure the safety and security of both physical and soft data files which are shared, (including, but not limited to, a safe location within the office where access is limited to authorized personnel only, physical barriers, metal locking cabinets etc.).
- If any part of the processes to be outsourced (collection, analysis, data storage) to private entities, ensure data storage location is defined, and applicable laws governing data management and disclosure are known and reflected in agreements and contracts.
- Assess the right methodology to use, including best data collection methods and who is best placed to collect the data.
- Assess risks regularly and design/adapt systems to ensure the systematic and consistent monitoring and assessment of evolving data protection threats and risks. Active monitoring as well as feedback from affected communities and data subjects will assist in these measures.
- Ensure data is stored in a safe location, where access is limited to authorized personnel only, (through access cards, physical barriers, locks, etc.)
- Determine appropriate access rights to data depending on responsibilities, needs and sensitivity of the data.
- Ensure system parameters are in line with principles, and not only from a technical point of view.
- Establish appropriate security measures for electronic and/or physical files, including but not limited to;

- Regulated access by authorized personnel only, file encryption, and/or password-protection;
- Minimize systematic passwords used for all kinds of IT equipment, (including portable devices, such as laptops and mobile phones;
- Ensure backups are rendered on a regular basis to prevent accidental loss or damage to data;
- Secure means of transferring data to other agencies/organizations (encryption, xml files, etc.) throughout the entire IM cycle;
- Establish a procedure to relocate (and, as a last resort, destroy) physical and electronic files in case of an emergency evacuation;
- Ensure procedures to safely transported data and information across checkpoints or frontlines;
- Defining appropriate measures to safeguard interviews, e.g. personally identifiable data (PID) of interviewees and the information they provide kept separate from reports via standardized a coding system or other similar measure.

- Build feedback and complaints mechanisms so affected populations can report concerns about data security and violations of data collection, sharing or other data protection related concerns.

IMPLEMENT

- **Conduct Data Collection:** Systematic data gathering / collection based on defined purpose (step 5)
  - Ensure technical and organizational measures are in place to ensure the safety and security of enumerators, interviewees, physical and soft data files which are collected.
  - Assess risks regularly and design/adapt data collection approaches to ensure the safety and security of data collection throughout the lifecycle of the data collection initiative. Active monitoring as well as feedback from affected communities and data subjects will assist in these measures.
  - Ensure appropriate measures are in place to protect data, in particular sensitive protection data (including, but not limited to, personal data) against the risk of accidental or unlawful/illegitimate destruction, loss, alteration, and unauthorized disclosure or access, (including during transport and/or transfers of data).
  - At all times, be attentive to signs that the data collection activity may create risks, or that mitigation measures may be failing. As such, make sure to include ‘red lines’ or thresholds for any moment or situation that may require the immediate cessation of the project and the deployment of remedial or mitigation measures.
- **Process and Analyse:**
  - Identify and ensure adherence to the organization's data protection policies and guidelines on the processing of data collation, collection and analysis initiatives.

IDENTIFY DATA THAT HAS BEEN COLLECTED IN THE "GREY ZONE

  - Identify a staff member who is accountable for the policy's implementation and enforcement where appropriate.
  - Train all staff involved in handling sensitive information on data protection and security standards, skills, policies and principles. This includes the types of personal and sensitive data identified within the operation, (make sure these are documented and known to all).
  - Define appropriate measures to protect the user against privacy issues such as surveillance, inappropriate aggregation, exclusion, confidentiality breach, and increased accessibility, identification of individuals or groups, and secondary data usage.
- **Disseminate and Share:**
  - Ensure the decision to disseminate information publicly is based on a careful analysis of the risks and benefits, bearing in mind the data protection risks inherent to specific dissemination tools and platforms.

- Do not share data if the risk of harm is high. Data should only be shared if the risk of harm is low, measures are in place to implement the mitigation of this harm and you have sufficient information to make an informed determination on the level of risk.

❖ **Store and Maintain:**

- In the context of personal data, beneficiaries should have the right to access their own information without undue delay or expense, and in a format which is meaningful to them.
- Define clear procedures to establish data ownership/control/hosting/management, and relevant rights of correction, deletion, archiving and destruction of all storage and maintenance
- Define a classification system(s) to tailor protocols based on sensitivity assessments (e.g., by ranking the potential harm as low, moderate or high)
- Draft a master list of who has access to which information and any needed authorizations.
- For physical files, maintain lockable filing cabinets, limited access to these files to authorized personnel and adherence to any and all data protection policy or other guidelines on the processing of data.
- Establish appropriate security measures for electronic and/or physical files, including but not limited to:
    - Regulated access by authorized personnel only, file encryption, and/or password-protection;
    - Reset passwords systematically used for all kinds of IT equipment (including portable devices, such as laptops and mobile phones) on a regular basis.
    - Ensure backups are rendered on a regular basis to prevent accidental loss or damage to data;
    - Establish procedures to relocate – and, as a last resort, destroy – physical and electronic files in case of an emergency evacuation;
    - Defining appropriate measures to safeguard interviews, e.g. personally identifiable data (PID) of interviewees and the information they provide kept separate from reports via standardized a coding system or other similar measure.
    - Build feedback and complaints mechanisms in place so affected populations can inter alia, report concerns about data security and report violations of data collection, sharing or other codes of conduct concerns.
    - For physical files, maintain lockable filing cabinets, limited access to these files to authorized personnel and adherence to any and all data protection policy or other guidelines on the processing of data.

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

ACCESS INFO LANDSCAPE

- **Define Information Needs:**
  - Ensure that defined information and data needs are grounded along the lines of defined purpose, proportionality and the need to establish facts necessary for an informed protection response.
  - Apply a holistic approach that includes all relevant segments of the population, locations, and risks. Identify potential biases of all relevant segments that may be present.
  - Rely on evidence-based information & facts and informed assumptions to ground understanding/decisions as the main tool to ensure impartiality.
  - Ensure transparency and consultation with all relevant stakeholders (including re-evaluating information needs based on findings) is practiced from data collection to analysis in all aspects of PIM with clearly defined SOP's outlining defined purpose (data and info needs) methodology, roles and responsibilities, from the onset of any PIM activity.
- **Data and Information Review:**
  - Ensure that the criteria for SDR are clearly stated, up to date, unbiased and that the sources of the data and information are objective, and documented.
  - Data and information should be assessed/triangulated based on reliability of the source, where possible as well as credibility, contextualization of the information, methodology used to produce the information, and potential inherent biases noted from any given source. Data should either be accepted through collaborative process with partners and stakeholders or excluded from the SDR.

DECIDE AND DESIGN

- **Information Sharing:**
  - Ensure that procedures for information collection and sharing within the community of stakeholders are coordinated, impartial, transparent, documented and shared.
  - Work to ensure impartiality by reaching out to all relevant stakeholders, through established and mutually agreed protocols for information collection, sharing and review.
  - Agree on the uses and parameters of shared data and information jointly collected, i.e. shared data and information may only be used transparently, used within the parameters agreed for of responsible interpretation and for specific defined purposes which will benefit the population of concern.
  - Establish agreement on how the community of stakeholders may respond to or mitigate identified bias, i.e. possibly sharing the data or information, or by agreeing to share identified bias or other limitations in a transparent manner in the methodology, this ensures also the consistency in the use of the data and possibility to replicate the process. Accompanying, for example a final analysis or any interpretation or use of the data.

.

- **Design with Affected Population:**
  - Be aware of and mitigate situations which may lead to the exclusion of persons of concern based on timing, language ability, etc.
  - Work with the population of concern to identify areas of potential bias which may affect how they engage with colleagues within the humanitarian community, especially in the context of shared data collection exercises.
  - Test questionnaires with members of the population of concern to check and ensure that there are no leading questions, hidden bias or misinterpretation issues in data collection questions or questionnaires.

- Work with stakeholders in the humanitarian community to define and disseminate transparent messaging around the purpose, scope and use of any data collection exercise well before its start.
- Ensure staff working with persons of concern are well informed of, and deliver a consistent and uniform message on the scope and intended results of the data collection exercise- managing expectations around intended outcomes. Test messaging within the community for understanding, before proceeding.
- Report abuse of authority and situations where staff may be acting in an unethical, impartial or non-objective manner- include in messaging to persons of concern (and staff) clear instructions on how the population of concern (or staff) may complain and to whom, including how complaints will be dealt with (i.e. in a confidential manner). As appropriate provide feedback and dialogue with persons of concern on complaints lodged. Test messaging within the population of concern for understanding, before proceeding.

❖ **Design Information System:**

- Jointly review and set up protocols with members of the humanitarian community (including national actors and other stakeholders as appropriate) prior to the start of a data gathering exercise. This also ensures consistency in review and possibility to replicate the process.
- Set up safeguards by outlining all objectives and outputs of a given system based on an objective assessment of defined purpose.

Reflect on and mitigate potential bias of the assessor in data gathering.

- Provide proper interpretation guides for data collection, which may minimize room for wrongful interpretation by assessors.
- As a community of responders, identify and be aware of specific cultural, social, economic, political or other factors which may result in bias, lack of transparency or impartiality check this against your data collection plan.
- Rigorously review your data collection plan ensure that it is result oriented and that the method information is collected in is credible.
- Train assessors to cross-check and review for bias, follow prescribed methods. Ensure that enumerators are well trained and abiding by the code of conduct, through periodic review and feedback from persons of concern.
- Tools are aligned with the intended purpose, tool is built in a way to minimize unbiased responses, for example: look for misleading questions, leading questions or issues with the questionnaire which could result in bias.

IMPLEMENT

❖ **Conduct Data Collection:**

- Observations will need to be included in the final analysis and depending on the scope and type of situation may need to be factored into ongoing data collection.
- Throughout data collection, data collectors must ensure that the response of those interviewed respondents are correctly captured and allows the respondent to "not give an answer to a question"
- Consistently revisit the ethical or responsible process or implications of the data that you are collecting (throughout the data collection cycle- for example cease data collection if concerns become apparent).

❖ **Process and Analyse:**

- Avoid letting partial understanding of context influence validation of analysis results. Reflect over use of expert knowledge or judgment.
- Develop a plan for timely and accurate data analysis plan and to avoid misinterpreting results.
    - Vet aspects of the analysis, and assumptions made on expert knowledge with key subsets of the population of concern.
    - Ensure an impartial and unbiased process through establishing protocols and a replicable process for analysis.
    - Establish protocols for analysis based on a transparent and unbiased data analysis plan, which will also make the results replicable.

- Ensure documentation of analysis, decisions, assumptions and limitations are transparent.
- Work with the community of stakeholders to recognize analytical limitations and vet or triangulate findings in an impartial and transparent manner.

❖ **Disseminate and Share:**

- Work with the humanitarian community to vet incoming requests for data and information, ensuring these requests are of an impartial, unbiased nature and centre on a commonly agreed defined purpose, which is proportional and will deliver protection results on behalf of persons of concern- while also reflecting the other PIM Principles.

❖ **Store and Maintain:**

(nothing)

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 the social demographic and cultural context.

ACCESS INFO LANDSCAPE

- **Define Purpose and Information Needs:**
  - Reach out to affected people to understand their situation, vulnerabilities, threats and capacities and the resulting data and information needs, timing, scope and format of data or information needed.
  - Identify data disaggregation needs by age, gender, diversity, specific groups within the social-cultural context
  - Identify preliminary data and information needs for protection strategy and response, based on concerns raised by the affected population
- **Data and Information Review:**
  - Analyse and triangulate existing data sets to identify consistencies and inconsistencies; relevance and reliability; overlaps and gaps; baseline and secondary data. Identify reliable data sets and ensure primary data collection tools do not collect this information again unless needed.
  - Identify both best and bad practices related to social and cultural sensitiveness in selection of secondary data to be reviewed.
  - Include data and information from affected population protection networks, systems, local organizations.
  - Understand (or note limitations in data or knowledge; identify reason for the gap) surrounding threats, vulnerabilities and capacities of protection risks within a certain group, by contrasting against the broader affected community; including for people of different ages, gender and background.
  - Maintain a risk assessment including internal, external and persons of concern, update and reflect changes in the situation and reflect data disaggregation accordingly.

DECIDE AND DESIGN

- **Information Sharing:**
  - Seek agreement on information sharing practices and processes preferred by the affected population, including for identifiable and anonymised data (including sharing with the community / community leaders, etc.)
  - Consult and identify if and how the affected population would prefer to receive feedback results and findings of PIM activities
  - Identify timing, scope, format and organizational responsibility/roles in terms of data and information to be shared with the community (based on outcomes of the above and protection best practices)
- **Design with Affected Population:**
  - Work with the community to ensure participation of people of risk at all stages of planning and programming, seek dialogue with different groups of people across age, gender, diversity, geographic locations, different status and needs.
  - Ensure accountability mechanism established and clearly communicated to affected population including the timing, scope and organizational responsibility for communicating/feeding back community identified (protection) data and information needs.
  - Identify and use existing community-based information sharing mechanisms and support them (especially those which facilitate information sharing among persons for their own protection) and build these capacities within the community
  - Ensure evolving contextual, social and cultural considerations are identified through linkages with the community of concern, and apply to identified data needs and adjust responsively.

- **Design Information System:**
  - While designing data collection tools, ensure to integrate information on community-led protection initiatives, mechanisms and capacities (not just protection risks/threats).
  - Survey design specialists and translators should work with members of the local community and carefully field test data collection tools to ensure questions, phrasing, and order of questions respect local culture and can be understood by community.
  - Ensure enumerators are trained and appropriate to the context and population they will be collecting data from.
  - Take into consideration cultural and social aspects regarding time and place for interviews (i.e. daily working time and celebrations; inaccessible places for determined categories limiting physical and/or social access, etc.)
  - Define tools and methodology in order to reduce bias when capturing information on and from different groups of people in the community (e.g. age; gender; diversity; vulnerabilities; social, political, religious, economical background)
  - Where possible, include in SOPs details on proper recording and response to requests of persons of concern to access information, seek correction or deletion of their own data. Ensure the community understands when this will not be possible to modify (i.e. where data is being collected anonymously).
  - Design information system to reduce likelihood of an unequal power relationship (explicit or implicit in the way the exercise or the organisation carrying it out is presented) between the data collector and the data subject.
  - Train enumerators e.g. cultural sensitive data collection methods, communication on purpose and ways to manage expectations

IMPLEMENT

- **Conduct Data Collection:**
  - Clearly communicate the purpose of the exercise to the person providing their data (including the relationship of answers to aid and assistance provision to avoid raising / manage expectations), and to allow them to actively participate, and ask questions in a manner that respects person's cultural background; the person's freedom to answer them as they wish; but also to support complementary communication initiatives led / driven by the communities themselves.
  - Inform affected population to whom the information will be shared and disseminated.
- **Process and Analyse:**
  - Work with the affected population to assess and analyse protection related implications to this process step.
  - Recurrent review and update of the risk assessment, operationalize do no harm principles (as described in this document) and update the stakeholder analysis.
  - Analysis of disaggregated data should be by identified age, gender and diversity.
  - Present and discuss preliminary results with members of the community and integrate their interpretations and comments in the final analysis.
- **Disseminate and Share:**
  - Work with the community to update a risk assessment – re-examine changes in context, based on levels or types of data to share (as agreed in 'Information Sharing' step.
  - Ensure disseminated data is appropriately anonymised and aggregated (identifiable features removed).
  - Ensure data and information is shared in a timely, appropriate, accessible and predictable manner and maintain a dialogue with the community.
  - Use existing community-based information management mechanisms and support those to share feedback or relevant protection information.
  - Re-examine the communities evolving need for certain sets or levels of protection (and other) information, which they may need to make decisions for themselves and their families, and understand the timeframe for this information
- **Store and Maintain:**

- Where possible, affected people are aware of their right to access, and have access to stored data and information, which they have provided about themselves and are informed in cases where this will not be possible.
- Ensure data storage, retention, and destruction policies and procedures are in place that are relevant to the context / nature of the data / local laws / etc. and the community is consulted and informed of them.

Coordination and collaboration: All actors implementing PIM activities must adhere to the principles noted above and promote the broadest collaboration and coordination 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.

ACCESS INFO LANDSCAPE

- **Define Purpose and Information Needs:**
    - Map key actors, their initial priorities, information needs, protection and IM capacities, and existing initiatives to identify possible overlap and opportunities for collaboration, in consultation with relevant actors. This could result in a stakeholder analysis.
    - Reach out to and build linkages with sectoral stakeholders to understand what protection data and information may be needed for sectoral purposes.
    - Take into account broader information management environment - identifying risks and opportunities for collaboration.
    - Assesses various stakeholders and initiatives to identify information requirements and spot linkages
- **Data and Information Review:**
    - Identify and reach out to key stakeholders, including those essential to a coordinated protection response, to gather existing data, information, reports and other resources that are relevant to the identified information needs, and to become aware of ongoing or current data collection processes.

DECIDE AND DESIGN

- **Information Sharing:**
    - Verify credibility and reliability of existing data and information by consulting with data sources. If credible, work with data partners to put in place predictable measures to safely access, transfer and store data on an ongoing basis. Establish data sharing protocols or agreements as is necessary to assist in efficient and ethical sharing over time.
    - If coordination structures do not exist, discuss the need for and feasibility of setting one up with the community of stakeholders. Work with them to conduct a stakeholder analysis to identify potential participants or resources. The stakeholders involved will vary from context to context, and may include humanitarian actors, national authorities, civil society, development and peacekeeping actors.
    - If an information-sharing network is established, agree on its purpose, membership, modalities, standards (e.g., regarding data collection, analysis, use, access and dissemination), roles and responsibilities, and accountabilities.
    - Maintain coordination lists or communication platforms to facilitate networking and communication among the stakeholder community.
    - [[Ensure the partners' roles in the PIM are determined by their technical expertise and ability to manage protection information. It is not because a partner is not involved in the data collection that it should not have another role in the PIM and use the information for assistance.]]
    - Ensure transparency amongst the multi actors engaged in the coordination and adhere to the key the PIM principles.
- **Design with Affected Population:**
    - Reach out to the community of concern (e.g., by setting up regular transparent and inclusive coordination and communication mechanisms) to understand their situation, context, needs and internal communication structures --

- Deliver clear messages as a humanitarian community, about who is doing what, where, how and why.
- Ensure coordinated feedback to the community of concern about the data and information that is collected from them by humanitarian actors.
- Support and strengthen community-driven coordination and communication mechanisms, as requested by the community.

❖ **Design Information System:**

- Consult stakeholders on possible common standards for data collection, transfer/dissemination, storage, and protection. This may include data-sharing agreements, SOPs, or terms of reference for coordination groups.
- Consult stakeholders on possible indicators and proxy indicators they may be able to provide data on, agreeing on modalities, format and scope of the information to be shared.
- A responsive manner.

IMPLEMENT

❖ **Conduct Data Collection:**

- Inform relevant actors of the purpose and logistical details of your PIM activity, to avoid potential logistical conflicts or disruptions.
- Share information about the observed situation and changes in the protection environment.
- Share expertise, knowledge of the data collection environment and materials to reduce costs for individual organizations implementing data collection and reduce risk.

❖ **Process and Analyse:**

- Reach out to actors to assist in the interpretation, validation and verification of the data analysis (findings), as appropriate.

- **Disseminate and Share:**
  - Undertake a risk assessment as a community and consult persons of concern to understand if there have been changes in the situation or context which might affect the desirability or feasibility of sharing information or certain types or levels of data (vis-a-vis previously-agreed plans)
  - Consider methods to track if and how the data, information or reports are used, and by whom (both by internal and external actors).

❖ **Store and Maintain:**

- Implement the data storage and maintenance systems as per existing agreements, including with regards to access for partners once data is stored or archived, and decommissioning and disposal procedures.

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.

ACCESS INFO LANDSCAPE

- **Define Purpose and Information Needs:**
  - Bring together a multi-functional team of IMOs, Protection and non-IM sector specialists when defining the information needs.
  - Ensure clarity and understanding of the humanitarian system, including sector specific considerations, phases of humanitarian response, programmatic cycles and data protection when defining information needs.
  - Analyse IM environment (threats, opportunity, strengthens, weaknesses) to inform appropriate methodology design and operational planning and undertake stakeholder analysis.
  - Mainstream local knowledge and 'social fabric' throughout the process.
  - Be familiar with all communities of practice (namely, protection and information management), principles, standards and frameworks which need to collaborate and build upon each other despite which discipline / expertise is yours.
  - Communicate protection and information needs clearly, and to focus data collection and information efforts around defined purpose, proportionality ensuring that data, information or analysis will be coordinated and shared as broadly as appropriate.
  - Ensure clarity on operational guidance is agreed to within the operation/region, (if not globally available), with respect to international principles, norms, standards (i.e. PIM results)
  - Analyse and ensure linkages on information needs, design of data / information gathering and M&E are well considered and with a logical base. Ensure periodic review (including learning and adjustment) the PIM strategy using the appropriate monitoring and evaluation techniques.
- **Data and Information Review:**
  - Conduct an initial workshop with all protection actors to discuss information needs, information gaps and how to fill them (PIM matrix to help guide the discussion). This should build from the initial dialogue from the first step. Identify and ensure the inclusion of all relevant stakeholders around the PIM principles.
  - Apply a community and rights based & participatory approach Protection and IM must have the competency and capacity to jointly review information sources, evaluate their reliability to ensure they are up to date, unbiased, and that the sources and their data & information are objective – (i.e. explanation of methods used to collect data / information.) and the objectives of the exercise clearly specified.
  - Analyse validity of methods, reliability, credibility and bias which can bring the analysis/data initiative to the closest truth possible. (Could also be used be in the data and information review step)
  - Ensure technical capacities are available, (data management skills, analytical skills for both quantitative and qualitative, system design skills, mapping etc.).
  - Ensure and validate findings of any and all analysis with local, entity which can provide local knowledge.
  - Ensure the criteria of an SDR is clearly stated and identified biases are communicated (i.e. either are accepted through collaborative process, or that set of data/information are excluded from the SDR. After SDR make an informed community led decision on which systems are needed based on a comprehensive analysis of information requirements (and over time).
  - Contextualize a vulnerably analysis, (i.e. be able to explain local vulnerabilities)

- Identify available data sources and partners, such as national actors, administrative data, judiciary data, justice sector etc.

DECIDE AND DESIGN

❖ **Information Sharing:**

- Build on the initial workshop of information needs and plans, define an appropriate data sharing mechanism to ensure appropriate collaborative measures.
- Protection sector to start sharing more predictably and transparently.
- Ensure any data sharing protocol respects both protection and IM standards and needs (these must be aligned).
- Disseminate and champion PIM products (representation and communication skills) at all stakeholder levels.
- Ensure decisions and approaches to disseminate, share, and establish linkages with sector partners are consistent with intended purpose. Ensure PIM activities and decision are regularly revisited as the context evolves. Agree a data sharing agreement conducive to the context.
- Consider both disaggregated and aggregated data. Communicate sensitivities around confidential information and work to establish agreements with stakeholders surrounding the sharing of critical protection data, information and analysis in a protection appropriate manner. (Reformulate)
- Ensure the initial kick-start of any PIM collaboration, include cross sector briefings which highlight what protection IM means within each sector. I.e. what does protection mean in WASH, Shelter etc. Protection Actors must also be ready to explain the PIM framework which is applicable to the given context (which purposes are driving the system landscape). Share these approaches. All protection actors should understand protection through the lens of other sectors.
- Ensure PIM related information and analysis coherently and coherent at different stages of the programme cycle, it should not be a one off. Define audiences of data and information sharing results.
- Explore and/or establish partnerships with other sectors and spot linkages for PIM systems with other processes. Keep people informed and communicate effectively and predictably with stakeholders, including the set-up of information sharing protocols and conduct privacy impact assessment or something similar.
- Engage the community of stakeholders, and disseminates lessons learnt and good practices with colleagues locally and globally to support sustainability and knowledge management.
- Proactively encourages engagement and contribution from partners to support PIM activities and communicates effectively with a variety of stakeholders. Internal and external colleagues and between technicians and decision makers, translate technical discussions for a non-technical audience.

❖ **Design with Affected Population:**

- Engage and communicate with communities in a responsible manner and is aware of AAP principles Understand and apply a community and rights based & participatory approach when designing a protection IM system.
- Define this in a SOP to explain to and engage with the population on all aspects of data collection initiatives and steps within the process.
- Engage in coordinated, meaningful and sustainable support, and collaborate with of community-led coordination mechanisms, as appropriate.
- Engage and communicates with communities in a responsible manner and is aware of AAP principles.
- Ensure the expertise in the effective design and implementation of data collection through interview, including in cross-cultural environments and complex security environments.
- Ensure existing sources of knowledge and a staffing plan is in place to engage local knowledge where appropriate.

❖ **Design Information System:**

- Balance all aspiration with feasibility as constrained by operational context and programmatic constraints.
- Make informed decisions on which systems are needed based on a comprehensive analysis of information requirements (and over time)
- Ability to plan and lead or participate in data collection- ensure that data collection is principled, safe and purpose defined through all steps.
- Tailor data collection techniques to a wide variety of situations, including low tech environments
- Design and develop appropriate sampling techniques, as well as quantitative and qualitative data collection methods including data collection design
- Design appropriate community mapping/target population methods
- Agree on a framework which identifies and contextualize in consultation with local actors (i.e. operationalize) relevant local and international norms and standards on data protection.
- Develop in consultation with relevant colleagues appropriate monitoring and evaluation techniques – including different types of indicators - and how to apply them to protection information management. As needed, draft technical documents to clearly articulate and scope IM systems and plans.
- Prioritize multiple and possibly competing deadlines and tasks around PIM activities Ability to troubleshoot/move to contingency plans as required
- Technical skills on interview techniques and different data collection processes
- Understanding of research ethics Cultural knowledge and understanding of the operational context Able to develop a principled PIM strategy and operational plan, and incorporate contextual risks, vulnerabilities and coping mechanisms within protection data analysis processes.
- Ability to use existing and new technological solutions for information management and able to assess their appropriateness for different contexts, including tailoring IM systems to low tech environments.
- Ability to tailor data collection techniques to a wide variety of situations, including low tech environments
- Knowledgeable of key protection norms and standards and a holistic approach of protection and the ability to incorporate these into operational and technical solutions Is familiar with appropriate mapping and sampling techniques, as well as quantitative and qualitative data collection methods including data collection design
- Familiar with the Project Management Cycle and has sound project management skills, including creating work plans, budgeting and delegation of responsibilities Is able to set clear milestones, organizing work accordingly and monitoring progress Is able to scope and manage expectations of IM
- Both protection and IM colleagues must take responsibility for the data and information requirements of requisite IM systems, including recording information in physical files &, adhering to data protection protocols. This is no longer solely the responsibility of technical colleagues. If there are limitations in capacity, these need to be identified and colleagues trained and held accountable.
- Ensure systems and HR capacity in place to store and process data / information.
- Assesses various stakeholders and initiatives to confirming information requirements Vis a Vis system approach

IMPLEMENT

❖ **Conduct Data Collection:**

- Elements above (in the definition) should be included in the how below).
- Engage and communicate with communities in a responsible manner and is aware of AAP principles
- Design and implement data collection through interview, including in cross-cultural environments and complex security environments
- Ensure backups taken on a regular basis to prevent accidental loss of or damage to data. In the case of data transfers, ensure does the organization have secure means of

transferring data to other agencies/organizations (encryption, xml files, etc.)? Ensure ail there a procedure is in place to relocate (and, as a last resort, destroy) physical and electronic files in case of an emergency evacuation

- **Process and Analyse:**
  - Engage and communicate with communities in a responsible manner and is aware of AAP principles
  - Keep people informed and communicate effectively with a variety of stakeholders
  - Ensure all the staff involved in handling and analysing sensitive information adequately trained on data protection and security standards, skills, policies and principles.
  - Aware of and able to ensure that measures are in place to protect the user against privacy issues such as surveillance, inappropriate aggregation, exclusion, confidentiality breach, and increased accessibility, identification of individuals or groups, and secondary data usage.?
  - Be able to work collaboratively with protection, IM and sectoral colleagues to process, analyze and arrive at results. Be familiar with the context / Experience working with displaced populations (including IDPs, refugees, asylum seekers, and returnees as well as civilians in areas of displacement) as well as a range of protection contexts, from emergency to protracted to return and recovery
- **Disseminate and Share:**
  - Results should be endorsed by the community of stakeholders contributing to the exercise or PIM systems.
  - Encourage engagement and contribution from/to and between partners to support PIM activities
  - Keep people informed and communicate effectively with a variety of stakeholders – internal and external colleagues and between technical specialists and decision makers, translating technical discussions for a non-technical audience.
  - Reference and apply humanitarian and protection principles
  - Uses quantitative and qualitative analysis as well as visualization methods, software and ability to produce and disseminate regular IM products tailored to appropriate audiences.
  - Able to clearly draft different types of technical documents.
- **Store and Maintain:**
  - Ensure systems and HR capacity in place to store and process data/information.