
5
5.1 PIM Sensitivities
5.2 Data Sharing
PIM Sensitivities

Package 5:

PIM Sensitivities and Data Sharing

What this package offers: This package sets out to improve participants' understanding of PIM sensitivities, and to strengthen their ability to manage and share data and information in a safe, responsible and purposeful manner in line with international norms and standards with regard to data protection.

Content:

Module 5.1: PIM Sensitivities (1 hour)
Module 5.2: Data Sharing (1 hour and 20 min)

Target group: This training package is suitable for groups of 10 – 28 participants with mixed functional profiles, with prior hands-on experience implementing and protection response and/or working with data and information for protection outcomes.

If delivered to a target group with no prior knowledge of PIM, it is highly recommended that this training package be delivered in conjunction with and after PIM training package 1 (PIM Foundation) or module 1.1 (Introduction to PIM Concepts).

Instructions for delivery:
While module 5.1 'PIM Sensitivities' can be delivered without module 5.2 'Data Sharing', the latter should always be preceded by module 5.1. Delivered as a package, the sequencing is that module 5.1 'PIM sensitivities' is delivered first, in order to equip the participants with a shared understanding the sensitivities around confidential information being handled. Module 5.2 'Data sharing' should be delivered afterwards, building off the knowledge acquired in module 5.1, by introducing international norms and standards with regard to data protection and exploring solutions to overcoming data sharing challenges within own operations.

While designed to be delivered as a package, the two modules may also be delivered in isolation, for target groups with a specific learning and interest in PIM sensitivities or data sharing respectively.

Time and preparation required: The preparation required by the facilitator for delivery of the modules themselves is specified under the respective module descriptions. In addition, as a prerequisite for the successful delivery of these modules, the facilitator should organize and request for participants to complete a pre-training survey, which the facilitator will use for the following:

- Be aware of the functional profiles and level experience of all participants prior to deliver (through pre-training event survey or registration questions).
- Be aware of participants experiences working with PIM Sensitivities to Data Sharing challenges and solutions.

Having knowledge of the above, will enable the facilitator, during the planning and deliver phases, to facilitate plenary discussion, which can be dynamic and enable the participants to reflect on their prior experience in relation to the subject matter discussed.

MODULE 5.1 - PIM Sensitivities

Core competency –
Knowledge: Understands the sensitivities around confidential information being handled.

Module objectives	Module learning outcomes
The session will: • Explain why data and information could be sensitive; • Explain what types of data and information could be sensitive; • Explain who could be at risk when managing (throughout the PIM Process) with sensitive data; • Discuss organizational and technical measures to address/mitigate risks associated with managing sensitive protection data and information	After the session participants will be able to: • Understand factors that could make data and information sensitive; • Distinguish between different data types, while detecting what could be sensitive data and information; • List who could be at risk in managing (throughout the PIM Process) sensitive data and information; • Relate organizational and technical measures to address/mitigate risks associated with managing sensitive protection data and information.

Key messages:
1. Sensitive protection data and information are data or information that, if disclosed or accessed without proper authorization, are likely to cause:
- Harm (such as sanctions, discrimination, retaliation) to any person, including the source of the information or other identifiable persons or groups; or
- A negative impact on an organization's capacity to carry out its activities or on public perceptions of that organization.

2. PIM sensitivities are contextual, temporal and relational. This also requires humanitarian practitioners to distinguish between different data types (i.e. personal and non-personal) and assess their sensitivities in an ongoing manner when there are changes in the situation or context).

3. When working with data and information, humanitarian practitioners must set out to understand, identify and mitigate the sensitivities and risk associated with collecting, processing, analysing, storing and sharing data and information.

Duration: 1 hour
Reference: PPT: 5.1 PIM Sensitivities, Module learning sheet content: Data and information typology; Diagram on sensitivity of data and information; ICRC Professional Standards for Managing Data and Information for Protection Outcomes; list of key resources.

Facilitator preparation:
- Familiarization with resources listed in Facilitator note 1.
- Reminders of participants' responses in pre-training survey.

Room set-up:
- Tables of maximum 5 persons by each: no assigned seats, individuals can choose.
- PIM sensitivities "graffiti wall" (blank board or connected flip chart papers).
- Markers or crayons (enough for all participants to be able to use simultaneously).
- Diagram on sensitivity of data and information (projected or drawn on flipchart/white board) (See facilitator note 4).
- Flip chart/board for note taking during session.

Prints and handouts:
- Stickers (any colour, at least 5 for each participant).

- Module learning sheet (Annex 5.1.a). One for each participant.
- Module feedback form (Annex 5.1.a). One for each participant.

Time	Activity	Resources
20 min	**PIM sensitivities.** Activity (all) @tables → graffiti wall	
	Introduce module learning objectives, and distribute Module learning sheet. Recall that management of protection data and information often involves dealing with a number of sensitivities that are in the nature of protection work. Note that the objective of PIM is to "*Strengthen our ability to provide data and information on persons or groups in displacement situation **in a safe**, reliable, and meaningful way for evidence-informed action and quality protection outcomes"* and point out that this session will exploring the "safe" element of this objective. Ask participants to go to the blank "graffiti wall" and for the next 5 minutes to (without speaking amongst each other) populate it with words, images, and expressions of why they think PIM is 'sensitive'. Hand out stickers and ask participants to spend 5 minutes individually reviewing the wall and to put the stickers on the words, images, or expressions they believe are the five biggest concerns which their colleagues have identified. Debrief for 5 minutes, by asking why they chose the words that they did. Have a discussion on the reasons which stand out as most important.	PPT,p.1-3 Module learning sheet Graffiti wall Markers Stickers
10 min	**What makes data and information sensitive?** Plenary (listening+discussing) @tables	
	Explain that what makes data sensitive is not a universal given, but always depends on other factors. Sensitivity is: 1) Contextual: Depends on operational context, levels of aggregation, etc.; Same data may not be sensitive in one context, but may be in another. (e.g., ethnicity data in South Sudan (where conflict is along ethnic lines) vs. Honduras (where there is no ethnicity dimension to the conflict. What may not constitute sensitive data and information in one context may be sensitive in another). 2) Temporal: Data may not be sensitive now, but can become so later in the future, depending on changes in the situation…. 3) Relational: One data piece in and of itself may not be sensitive, but it can become so when it is combined with other data. Think about how data may be combined resulting in potential harm or increased sensitivity. Referencing the points brought out by participants in the graffiti wall, explain data and information typologies in relation to sensitivities (Facilitator note 2). Conclude with the message that defining what is sensitive data and information will always be contextual, temporal and relational. Therefor it is important that in each operation, colleagues determine what information can be sensitive and should be subject to heightened protection measures in its use and processing.	PPT,p.4 Flipchart
10 min	**Data and Information Typology.** Plenary (listening+discussing) @tables	
	Personal data, meaning data that can be used to identify a person may be pre-labelled by an organizational Data Protection Policy as "confidential data" and is bound by the individual's right to privacy in addition to risks of un-authorized sharing of such data.	PPT,p.5-6

	This term should however not be confused with the term "data sensitivity" (the more contextual and relative term worked with in this module), because personal data is not the only type of data which may be sensitive. In reality, because we are dealing with human data, it may all carry the risk of being personally identifiable and/or sensitive. Before collecting data or designing a protection information management system, humanitarian actors must determine what data will be required for a specific and defined purpose and what the level of sensitivity is around that data. Ask if any of the participants have experience conducting such assessment to determine data and information sensitivities (i.e. as a part of a Data Protection Impact Assessment or 'DPIA')? If yes, then ask the participant/s about whether they operated with any fixed data and information typologies in that process (soliciting examples)? Explain that several broad categories of data and information can be identified, which have different levels of sensitivity in general and depending on context (See Facilitator note 3 for details) (Write or have pre-written the headings on a flipchart where they can be seen by the participants). ● Protection data and information (hereunder distinguishing PII, CII and DII) ● Personal data ● Sensitive data and information ● Sensitive personal data ● Confidential data (pre-labelled categories) Conclude that in order to determine the sensitivity level of a data or information type, it is necessary to conduct a risk and benefit assessment and review it on a regular basis throughout the project or programme cycle, or when there is a significant change in the situation or context. Introduce and explain the diagram on sensitivity levels across data and information types (See Facilitator note 4). Explain that the more sensitive the data and information, the stricter the data protection rules and standards that will have to be applied, as illustrated in the diagram (categories of data often overlap).	Flipchart stand/paper/marker (for use during delivery or with headings pre-written). Diagram on sensitivity of data and information (projected or drawn on flipchart/ white board)
10 min	**Who can be at risk when managing sensitive data?** Plenary (listening+discussing) @tables	
	Ask participants 'Who can be at risk when managing data that is sensitive?' and facilitate the sharing of insights by participants. Summarize the discussion and conclude who can be at risk: - *The individual(s) whose data is collected.* - *The survivors or witnesses, for example reporting or recounting human rights abuses.*	PPT,p.7

	- The communities being monitored using community-level needs assessments or reporting methods. *- Other communities of persons of concern (there is a risk that if communities hear about service providers disregarding confidentiality or consent, it will disrupt help-seeking behaviour of others).* *- The humanitarian staff and/or organizations (for example Monitors obtaining and managing data and other staff in their organizations such as humanitarians in Rakhine state, Myanmar going in to do monitoring brought no pen or notepads, but had to remember their observations rather than to note them down, because it was too risky to be seen performing their work).* Highlight that data sensitivity and risk may be different in other steps of the PIM process, and that reflection and context-specific risk and benefit assessment is encouraged for each step of the PIM process. The document "PIM Principles in Action" developed by the PIM Working Group contains a number of recommended PIM principled actions for protection at large as well as data protection (Facilitator note 5).	
5 min	**Data protection & security measures.** Plenary (listening + discussing) @tables	
	Note that being aware of the risks associated with handling of sensitive data, begs the question: What can we do to mitigate or prevent the risks? Explain that we can distinguish between technical and organizational measures (see Facilitator note 6). If time allows: Ask if anyone has other examples? Conclude that appropriateness of measures depends on many things, e.g.: ● *Balance of risks vs benefits* ● *The sensitivity of the information* ● *Availability and cost of the required equipment* ● *Operational feasibility of implementing the measure(s)* ● *Etc.* Ask if participants are familiar with the ICRC "Professional Standards for Protection Work" (3rd ed. 2018) and explain that these contain general and specific standards for the management of personal data and sensitive data and protection information. These are listed on the Module learning sheet. Ask participants at which step of the process should measures be put in place to protect sensitive data? Based on answers provided, conclude and explain: • *Measures should be in place before any data collection or sharing at the DESIGN stage (Step 2 of PIM Process), along with the identification of what data is sensitive in the context of the activity.* • *More about how to actually do this will be covered in the Module on Data Sharing, in particular with respect to the steps for conducting the benefit and risk assessment.*	PPT,p.8-10
5 min	**Summary.** Plenary (listening) @tables.	
	Summarize the module key messages (see module description) by reference back to the issues that came up during the Graffiti Wall exercise, and answer any questions necessary to ensure that module learning objectives have been met.	PPT,p.11-12

	Instruct participants that their Module learning sheet contains space on which they can add their notes and check out the list of resources. Project the "Moment of Zen" (2:10 min, "Do you know what happens your sensitive data?" by European Digital Rights: https://www.youtube.com/watch?v=GsFHfzmJQjA). Distribute module feedback form (one per participant) and collect the filled in version from participants before module closure.	Projector, speakers and internet Module feedback form (Annex 5.1.a)

Facilitator note 1) Recommended readings

GovLab (2016): Mapping and Comparing Responsible Data Approaches, available at: http://www.thegovlab.org/static/files/publications/ocha.pdf

Harvard Humanitarian Initiative: Signal Code, A Rights-Based Approach to Information in Crisis, available at: https://signalcode.org/

Terre des Hommes (TdH) and CartONG (2018), "Data Protection Starter Kit", available at: https://www.mdc-toolkit.org/data-protection-starter-kit/

International Committee of the Red Cross (2013, 3rd edition forthcoming in 2018): Professional Standards for Protection Work, Chapter 6 "Managing Data and Information for Protection Outcomes", available at: https://www.icrc.org/en/publication/0999-professional-standards-protection-work-carried-out-humanitarian-and-human-rights

International Committee of the Red Cross and Brussels Privacy Hub (2017): Handbook on Data Protection in Humanitarian Action, available at: https://shop.icrc.org/handbook-on-data-protection-in-humanitarian-action.html?___store=default

Office for the Coordination of Humanitarian Affairs (OCHA) (2016): Building data responsibility into humanitarian action, available at: https://reliefweb.int/sites/reliefweb.int/files/resources/TB18_Data%20Responsibility_Online.pdf

PIM Common Terminology (2018 ed.), available at: http://pim.guide/wp-content/uploads/2018/04/Protection-Information-Management-Terminology_Revised-Edition-April-2018.pdf

PIM Working Group (2017): PIM Principles in Action, available at: http://pim.guide/guidance-and-products/product/pim-principles-action/

PIM (2018): A Framework for Data Sharing in Practice: http://pim.guide/wp-content/uploads/2018/05/Framework-for-Data-Sharing-in-Practice.pdf

Responsible Data Forum (2016): The Handbook of the Modern Development Specialist – Being a Complete Illustrated Guide to Responsible Data Usage, Manners and General Deportment, available at: https://responsibledata.io/resources/handbook/

Tactical Technology Collective (TTC) and Front Line Defenders (2016): Security-in–a-Box, available at: https://securityinabox.org/en/

United Nations High Commissioner for Refugees (UNHCR) (2015): Policy on the Protection of Personal Data of Persons of Concern to UNHCR, available at: http://www.refworld.org/docid/55643c1d4.html

WHO (2007): Ethical and safety recommendations for researching, documenting and monitoring sexual violence in emergencies, available at: http://www.who.int/gender/documents/OMS_Ethics&Safety10Aug07.pdf

Facilitator note 2) What is "sensitive data and information"?

- *Sensitive protection data and information are data or information that, if disclosed or accessed without proper authorization, may cause:*
  - *Harm (such as sanctions, discrimination) to any person, including the source of the information or other identifiable persons or groups; or*
  - *A negative impact on an organization's capacity to carry out its activities or on public perceptions of that organization.*
- ***Disclosure** could be through voluntary or involuntary un-authorized misuse e.g. through accidental or unlawful/illegitimate destruction, loss, theft, disclosure alteration, copying, unauthorized used or misuse, use, modification/contamination, and unauthorized access, use or disclosure.*
- ***Harm/Risk**: Can be created by both action and inaction. Results in:*
  - *Aggravate existing threats, or create new ones;*
  - *Increase existing vulnerabilities, or create new ones;*
  - *Weaken existing capacities, coping mechanisms and/or self-protection strategies;*
  - *Trigger the resort to negative coping mechanisms;*
  - *Diffuse the threats to new groups/communities who were previously not at risk.*

Facilitator note 3) Data and information typologies

a. Data and information

'Data' means a collection of facts, such as numbers, measurements, or observations, whereas 'information' means facts or details about a subject.

(Source: PIM (2016): Commonly used Protection Information Management Terminology, available at: http://pim.guide/wp-content/uploads/2017/01/Commonly-used-Protection-Information-Management-Terminology_June-16.pdf)

b. Protection data and information

Data and information pertaining to protection risks/issues and situation of specific individuals/groups.[1]
We can largely distinguish between:

- Personal Identifiable Information (PII): which can lead to identification of an individual.
- Community identifiable information (CII): which can lead to identification of a community.
- Demographically identifiable information (DII): which can lead to identification of specific demographic entity.

(Source: PIM (2016): Commonly used Protection Information Management Terminology, available at: http://pim.guide/wp-content/uploads/2017/01/Commonly-used-Protection-Information-Management-Terminology_June-16.pdf)

What is personally identifiable data vs. non-personally identifiable data?

The current definitions of personally and non-personally identifiable data continue to be challenged by modern technology. Because we are dealing with human data, it may all carry the risk of being personally identifiable. It is recommended to instead focus on how to prevent harmful use and how to assess risk through the operationalization of a shared risk and benefit assessment. Doing so can clarify the actions needed to assess or prevent risk, based on a series of steps. The shared analysis of the risks and benefits for a particular data sharing process would then be the component of this process that is shared.

[1] Commonly used Protection Information Management Terminology; p. 42, available online here: http://pim.guide/wp-content/uploads/2017/01/Commonly-used-Protection-Information-Management-Terminology_June-16.pdf, accessed 5 March 2018.

(Source: PIM (2018): A Framework for Data Sharing in Practice, available here: http://pim.guide/wp-content/uploads/2018/05/Framework-for-Data-Sharing-in-Practice.pdf)

c. Sensitive protection data and information

Sensitive protection data and information is data or information whose disclosure or unauthorized access is likely to cause:

- harm (such as sanctions, discrimination, repression or stigma) to any person, including the source of the information or other identifiable persons or groups; or
- a negative impact on an organization's capacity to carry out its activities, including due to reputational damage.

Sensitivity of data is defined in relation to the particular context, and the level of aggregation and may change over time. Therefore, the same data may not have the same level of sensitivity in different contexts. Protection data and information that does not contain personal data may nevertheless be sensitive. It may relate to communities and other groups, to anonymous individuals, or to specific events or issues. In armed conflicts and other situations of violence, various aspects relating to the humanitarian, human rights, political or security situation may exacerbate the risks to people.

Likewise, aggregated or pseudonymized data may still be sensitive. Individuals or groups may still be identifiable, especially depending on the location and sample size, and thus may be exposed to harm if data about them is disclosed. It is therefore not possible to propose a definitive list of what types of data or information constitute sensitive information. However, some key types of information may belong to this category, including information about the nature of violations affecting specific individuals or groups, details about victims and witnesses, the affiliation of perpetrators, operational details related to military operations or security, etc.

Recognizing that the privacy, security and integrity of individuals or groups may be put at risk even if no personal data is collected and processed, protection actors as a matter of best practice apply the standards derived from the principles of data protection to sensitive data and information used for protection purposes, to the extent that it is necessary given the particular sensitivity of the data.

(Sources: International Committee of the Red Cross (2018, 3rd edition forthcoming): Professional Standards for Protection Work, Chapter 6 "Managing Data and Information for Protection Outcomes").

d. Personal data

Personal data, also known as personally identifiable information (PII), is data relating to an identified individual or to a person that can be identified from that data, from other information or by means reasonably likely to be used related to that data. This could include, for instance, an identifier such as a name, an identification number, location data, audio-visual material, or an online identifier. Personal data also include: country of asylum, individual registration number, occupation, status, religion and ethnicity. And it includes biometric data such as a photograph, fingerprint, facial or iris image, as well as any expression of opinion about the individual, such as an assessment of their legal status and/or specific needs.

(Source: PIM (2018): A Framework for Data Sharing in Practice, available here: http://pim.guide/wp-content/uploads/2018/05/Framework-for-Data-Sharing-in-Practice.pdf)

e. Sensitive personal data

Sensitive personal data are personal data that, if disclosed, are likely to result in harm (such as discrimination) for the individual concerned. As a result, many of the international instruments on data protection mentioned in this chapter include stricter rules for the processing of sensitive personal data. Given the specific situations in which protection actors work, and the possibility that some data could give rise to discrimination, setting out a definitive list of categories of sensitive personal data in protection contexts is not meaningful. Sensitivity of data and appropriate safeguards (e.g. technical and organizational security measures) will be context-dependent and may change over time within a given context; therefore, they need

to be considered on a case-by-case basis. Data relating to health, race or ethnicity, religious/political/armed group affiliation, and genetic and biometric data are considered to be sensitive personal data at all times. The nature of violations and abuses affecting specific individuals or groups, and the identity of perpetrators and witnesses, also fall into this category. All sensitive personal data require additional protection even though different types of data falling within the scope of sensitive data (e.g. different types of biometric data) may present different levels of sensitivity.

(Sources: International Committee of the Red Cross (2018, 3rd edition forthcoming): Professional Standards for Protection Work, Chapter 6 "Managing Data and Information for Protection Outcomes").

f. Confidential data (pre-labelled categories)

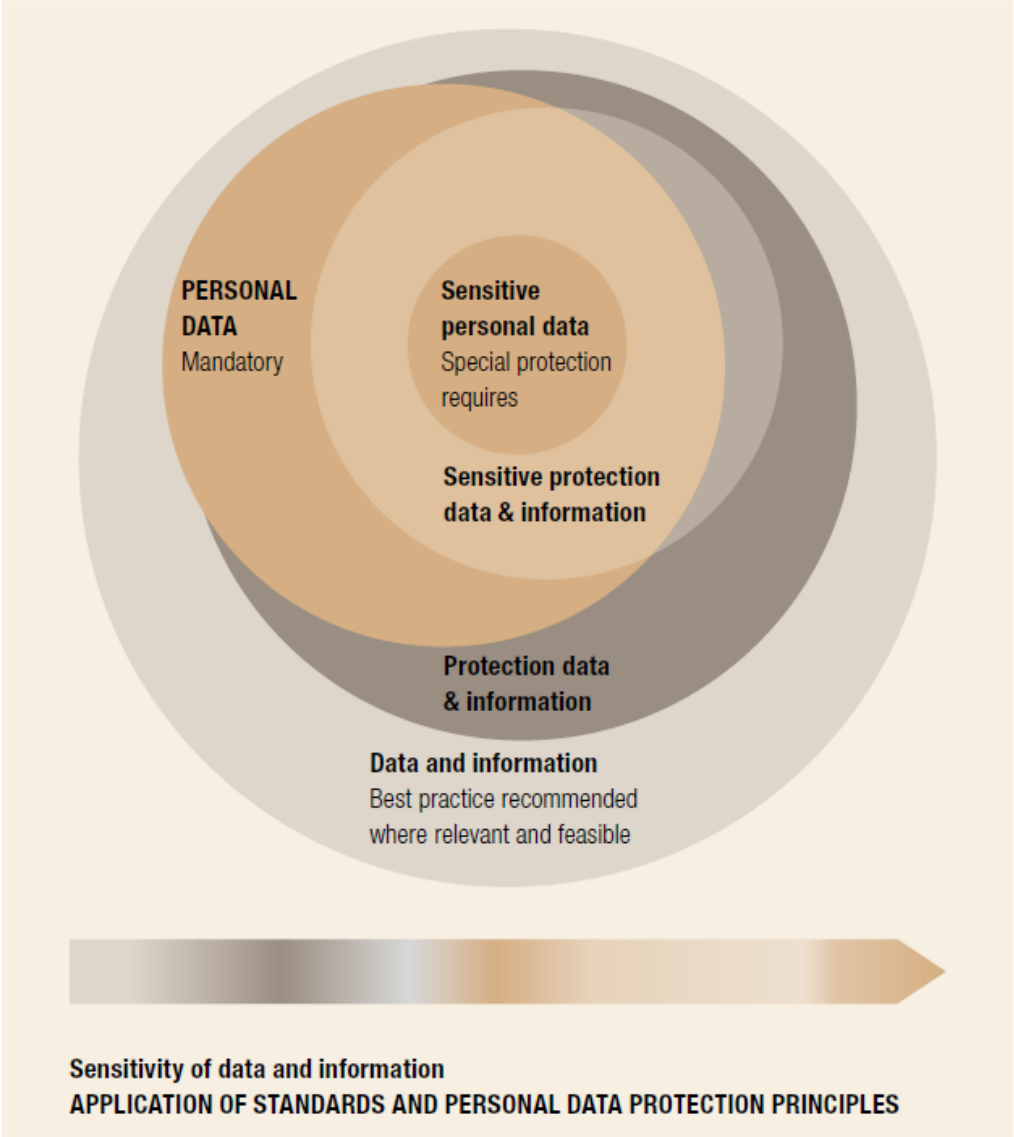
Confidential data is data for which will not be disclosed or otherwise made available to unauthorized persons or entities in ways that are inconsistent with the understanding of the original disclosure or without prior consent. There is an obligation to exercise utmost discretion with regard to all matters. Information known shall not be communicated to any Government, entity, person or any other source, nor made public.' (UN Staff Rules and Regulations (e.g. Regulation 1.2.g.) Information received from sources and clients will only be used and/or shared for specific purposes only when the person in question has provided specific and informed concern to do so. (OHCHR Code of Conduct). Even if consent for the use of information is given, the potential implications of that action for the safety of the person providing the information and of other people involved in the situation (e.g., the family of witnesses) must be assessed. If there is a risk of endangering any of them, the information should not be disclosed or in a manner that removes the risk. The safety of victims, witnesses and other cooperating persons must be a paramount concern; confidentiality as a measure to protect their safety should therefore take precedence over other considerations.

(Source: Office of the High Commissioner for Human Rights (2001): Manual on Human Rights Monitoring, OHCHR, p. 6, available at: http://www.ohchr.org/Documents/Publications/Chapter02-MHRM.pdf).

Facilitator note 4) Diagram on data and information sensitivity

The below diagram from ICRC illustrates sensitivity and the relationships between types of Data and Information explained in the above Facilitator note:

Diagram: Relationships between types of data and information



(Source: International Committee of the Red Cross (2018, 3rd edition – forthcoming): Professional Standards for Protection Work, Chapter 6 "Managing Data and Information for Protection Outcomes")

Facilitator note 5) Principled action for data protection

The "PIM Principles in Action" document provides practical examples of application of the PIM Principles throughout the steps of the PIM Process, including guidance and advice from a protection and IM perspective. It is available here: http://pim.guide/wp-content/uploads/2017/01/PIM-Principles-in-Action - 2017.pdf

Key "Do"-recommendations from the document include:

- *Conduct a contextual risk assessment and do-no-harm analysis to identify risks, opportunities, legal and ethical issues related to data collection, processing, analysis and dissemination.*

- *Only collect and share personally identifiable data if 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.*

Example: Before sharing data or information benefit and risk assessment would need to be conducted, only when the benefits outweigh the risk and are proportional to the anticipated outcomes should sensitive data or information be shared. If it is found that sharing it would entail a significant risk, which outweighs the benefit– e.g. in the mixed migration context of Libya – choosing to not record the point of entry into the country of unaccompanied minors).

- *Collecting or using data and information only based on informed consent of data subjects, again see the Facilitator note 3 above, which details what informed consent means.*
- *Include safeguards to preserve the privacy, confidentiality and security of personal information in accordance with data protection and collection standards.*

Examples: Coding of data, pseudonymization.

- *Brief involved staff to ensure a shared understanding of purpose and risks*
- *Develop a data storing plan based on protection principles. Dispose of data once consent is expired and there is no longer use.*
- *Develop data sharing protocols, policies and procedures with a particular focus on protecting personal and sensitive data.*

Example: generic email addresses, which do not allow for personal identification of the staff who has communicated (e.g. sharing information about a human rights violation).

Facilitator note 6) Data protection & security measures

Measures should be in place before any collection or sharing of sensitive data, and may include:

1) *Technical*
    - *Changing passwords*
    - *File encryption*
    - *Data coding, pseudonymization, and anonymization*
    - *Offsite servers*
    - *Classification systems tailored to sensitivity levels*
2) *Organizational*
    - *Privacy Impact Assessments (PIA) and Data Protection Impact Assessments (DPIA)*
    - *Data sharing agreements Policies on data-handling and storage*
    - *Data-sharing protocols (and standard templates)*
    - *SOPs, checklists and guidance*
    - *Governance mechanisms for accountability in responsible data management*
    - *Staff capacity*
    - *Codes of conduct*

Appropriateness of measures depends on many things, e.g.,

- Balance of risks vs benefits
- The sensitivity of the information
- The availability and cost of the required equipment
- The operational feasibility of implementing the measure(s)

ANNEXES TO MODULE 5.1

Annex 5.1.a) Module learning sheet: PIM sensitivities

Part of module: 5.1 PIM sensitivities

Instructions for production and use: The module learning sheet should be printed one for each participant serve as learning reference point for the participants throughout and after the module. It contains structured

space for note taking on key concepts introduced, contains reference tools, definitions and a list of recommended resources for further learning.
Print out available:
https://drive.google.com/file/d/1WQlRzbBVWLH7i3PAyxohuXpVnaVjtQZY/view?usp=sharing

Annex 5.1.b) Feedback form: 5.1 PIM Sensitivities
Part of module: 5.1 PIM sensitivities
Instructions for production and use: The standardized and anonymous feedback form should be handed to participants after completion of the training module (one for each) for immediate completion and return to the facilitator, in order be used by the facilitator to evaluate the extent to which the module learning objectives have been met through realization of the module learning outcomes. The form will take 3-5 minutes to complete.
Print out available: https://docs.google.com/document/d/1xw89rIKeatQJWrqspLfn_Yx7R9Doh6LsYZS2aC-j05M/edit?usp=sharing

Annex 5.1.c) Power point presentation
Part of module: 5.1 PIM sensitivities
Instructions for production and use: This power point presentation may serve as visual reference during delivery of this module. Please note that facilitators are discouraged from rely sole on the power point presentation as visual reference during module delivery, as this is not compatible with the participatory design of the PIM training modules.
Available at:
https://www.dropbox.com/s/aou1qzok9frzvxy/PPT_Package%205_Module%205.1_PIM%20Sensitivities.pptx?dl=0

MODULE 5.2 - Data sharing

Core competency –
Knowledge: Is familiar with international norms and standards with regard to data protection.

Module objectives	Module learning outcomes
The session will: • Explain why we share, the benefits of sharing (safely, responsibly, and purposefully), and what and when we share; • Examine three spheres of challenges to data sharing through benefit-risk assessment dilemmas; • Explore the '*Framework for Data Sharing in Practice*' aimed at promoting and facilitating safe, responsible, and purposeful sharing.	After the session participants will be able to: • Explain safe, responsible, and purposeful data sharing; • Contrast challenges to data sharing through benefit-risk assessment dilemmas; • Devise solutions to overcoming data sharing challenges by drawing on the '*Framework for Data Sharing in Practice*'.

Key messages:

1. Safe, responsible and purposeful sharing of data, information, analysis and knowledge, enables stronger, evidence-informed, and comprehensive protection outcomes and humanitarian responses;
2. Information-sharing networks and agreements should be established early *before* any data is collected, shared and used. Colleagues should be looking for, and assessing the needs of key stakeholders and working to proactively share data and information with them in a timely, relevant and appropriate manner;
3. A context specific and joint 'benefit and risk assessment' aims to ensure that the benefits and risks of data sharing have been systematically and deliberately assessed prior to sharing, and that actions have been identified to maximize benefits and minimize risks.
4. The purpose of the *Framework for Data Sharing in Practice*' (hereafter the '*Framework'*) is to work toward an overall reduction of risk of sharing or not sharing and to illustrate the benefits of sharing through the use of a shared 'minimum' in terms of concepts, principles, methods and processes which can be built upon by colleagues within their specific context.
5. Establishing a shared minimum in terms of concepts, principles, methods and process. is as important as the final product, because it builds trust between actors while also creating pathways for collaboration and shared analysis.

Duration: 1 hour and 20 minutes (80 minutes)
Reference: PPT: 5.2 Data Sharing, Participant learning sheet**:** Introduction to OCHA & PIM (2018): *A Framework for Data Sharing in Practice*, links to relevant resources.

Facilitator preparation:

- Familiarization with key resources (Facilitator note 1), the dilemmas for use in the activity and content of the Module learning sheet.
- Ensure that participants are familiar with the PIM Process ahead of learning event attendance (e.g. by sharing it as pre-event reading).
- Summarize findings of pre-training survey for presentation during module: Adjust module content (for activity "Data sharing challenges and solutions") according to participants' responses in pre-training survey to the questions on experiences with data sharing (the results should be presented in anonymized form during the module, and feed into participants exploration of how to promote safe, responsible, and purposeful sharing in their own context. If this module delivered in conjunction with the IM module (2.2), then answers provided during the exercise on "challenges and solutions" under each step of the IM-cycle may also contain relevant answers from which to draw on.

Room set-up:

- Pre-positioned chairs of participants in semi-circle (horse shoe) facing the wall area of the PIM Matrix (facilitator sitting in front of the matrix) – NO TABLES.
- Flip-chart stand and marker (for facilitator).
- Open space for a moving activity (the flipchart should be positioned nearby for debriefing note taking).
- By the open space: Visual reference to guiding questions for dilemma discussion activity (i.e. flipchart or PPT slide).
- PIM Process illustration on wall to serve as visual reference point (poster/drawing) (Facilitator note 4).
- Visual reference to typology of sensitive data and information (left on wall from module 5.1).

Prints and handouts:

- Print outs (cutting into smaller sections required) of "What would you do if?" cards (Annex 5.2.a).
- Module learning sheet (Annex 5.2.b).

	Activity	**Resources**
	Introduction: Why, what and when do we share? Facilitator presentation @plenary	
	Introduce module objectives and learning outcomes. Distribute the Module learning sheet and explain that it contains information, note space and reference points which will be used during throughout this module. As necessary, recap the key learning points from module 5.1 PIM Sensitivities, in order for these to be fresh in the minds of the participants. Then proceed to open exchange on the below: **WHY share?** Initiate discussion in plenary on the question "Why do we share (data and information in the humanitarian sector)?". Ensure the conclusion is reached that: • *We share in order to improve decision making, in turn strengthening humanitarian responses and enhancing protection outcomes.* • *There is an ethical responsibility of data and information holders to share data and information in a safe, purposeful and responsible manner with actors who are in a position or have a responsibility to respond to issues raised.* **Sharing WHAT?** Ask if any of the participants can share an example of the types of data and information of **what** we (the humanitarian community) share. Ensure the conclusion is reached that: • *The humanitarian data which we share fall into three overall categories:* o *Context of the humanitarian crisis.* o *People affected by the crisis.* o *Response to the crisis.* Reference the data typologies of module 5.1 (Facilitator note 2+3 below) and briefly explain that **what** we share is:	PPT,p.1-9 Visual reference to typology data and information (from module 5.1)

	○ *Non-personal and non-sensitive data and information, personal data, sensitive personal data, protection data and information, sensitive protection data and information.* Note that: • *Data and information have different degrees of sensitivity.* • *Sensitivity is not universal but is rather determined based on temporal, contextual and relational factors;* • *Measures for data protection must correspond to the identified level of sensitivity.* **Sharing WHEN?** Ask participants **<u>when</u>** we share (data and information), and relate the answers given to the steps of the PIM Process (Facilitator note 4): • *Safe, responsible and purposeful sharing of data is not only the transactional act of passing (handing over) data and information.* • *The transactional act of sharing in and of itself is preceded by the establishment of information-sharing networks based on defined purpose(s), and an assessment of the reasons to share, both of which should be done early, before any data is collected, shared and used.* • *Firstly, assess the information landscape, i.e. define the purpose in relation to the data and information we are looking to share or to obtain.* • *Moving through the PIM Process, is an **iterative learning process,** which helps to ensure that your defined purpose is correct, and that you are asking the right questions around assessing the benefits and risks of sharing as you move through the steps of the PIM process.* • *Conclusion: Sharing should be a point of consideration throughout all steps of the PIM Process (Even though "Establish information-sharing networks" appears once as a sub-step in "Design", sharing should be a point of consideration throughout all the steps of the PIM Process).* Ask if any of the participants are familiar with the PIM Principle "Coordination and collaboration" (and if they can explain in their own words what this principle is about)? Ensure that the following point is made (either by participant or directly by facilitator): • *The PIM Principle "Coordination and collaboration" states that all PIM actors must "promote the broadest collaboration and coordination of data and information" and that "To the extent possible, PIM activities must avoid duplication of other PIM efforts and instead build upon existing efforts and mechanisms".* • *Sharing serves as an enabling factor for collaboration, avoiding duplication, loss of time, and waste of resources and burden on affected population.* • *Sharing also included the affected population - ensuring that they have the protection data and information that they need to make informed decisions for themselves and their families.* While the benefits of sharing in general are clear, it is also associated with both benefits and risks – which places us in dilemmas. The following activity will face us with some of these…	PIM Process visual reference point
	Data sharing 'benefit and risk' dilemmas. Activity (Pairs) @open space (standing activity)	
	Ask participants to stand up and to come to the open space, and to line up in two lines facing each other (the number of persons in each line should be the same, in order for each person will face a 'match' in the opposite line). Hand every couple of "What would you do if?" cards to each participant in one of the lines. Instruct participants to pair up with the person	PPT,p.10 "What would you do

	standing in front of them in the opposite line as a pair. Inform that the pairs now have 10 minutes to discuss their card's dilemma. 1. What was the dilemma? 2. Who were the parties involved? 3. What type of data and information did the dilemma concern? 4. What was the level of sensitivity of the data and information? (referencing the data typologies of module 5.1 PIM Sensitivities)? 5. What would be the benefits of sharing? 6. What would be the risks of sharing? 7. Would you share? Call for a 10 minute debrief in plenary (everyone standing in a circle, still in their pairs): Ask for examples from different pairs' dilemmas, debriefing on the questions discussion (devote most of the time and attention to question 5, 6 and 7). During the debriefing, take note of constructive suggestions made for how to tackle the dilemmas (these will be used as a point of reference for the next activity). Conclude by calling for reflection on the **risks of not sharing:** This is where we see duplication, assessment fatigue at best - and the loss of lives at worst. We have no way to assess how much harm we have actually caused by not sharing; but it is something to think carefully about especially in terms of an underlying ethical responsibility, i.e. how does not sharing critical data or information needed for decision-making caused direct or secondary harm?	if?" cards (Annex 5.2.a) Visual reference to typology data and information (from module 5.1) Flipchart stand/paper/marker
	Data sharing challenges and solutions. Facilitator presentation @plenary	
	Explain that although there can be risks associated with sharing, awareness of the challenges is the first step towards devising solutions. Explain that the PIM Working Meetings II & III – identified 3 spheres or types of data sharing challenges (See Facilitator note 5 for more details): 1. Practical and Procedural 2. Institutional and Structural 3. Mind-set and Trust Present the results of the participants responses to the pre-training survey questions that pertained to their experiences with data sharing challenges and solutions under each of the 3 categories (NB> This must be prepared by the facilitator ahead of the module, see section "Facilitator preparation" above). As relevant also reference the dilemmas discussed in the preceding activity. Identify the challenges most commonly pointed to by the participants, as a point of departure for discussion in the next activity. Refer to the solutions to data sharing challenges previously presented by the participants *(If this module is delivered in conjunction with the package the IM module, then recap the solutions to sharing of data identified in that module – otherwise inquire about participants experiences with solutions based on their answers to the pre-training survey – namely with finding solutions to data-sharing challenges (including the data protection and security measures that will have been discussed in Module 5.1 on PIM Sensitivities).* Based on these solutions, the participants may know the way forward on the challenges which they experience in their own contexts.	PPT,p.11-12 Summary overview of participants' reply to pre-training survey

	If not mentioned by the groups, point to the following as practices which hold promising potential with relevance for the humanitarian field (and on which participants can find more information in the Module learning sheet): - *Data Protection Impact Assessments (Facilitator note 6);* - *Data Transfer Agreements (Facilitator note 7).* - *A Framework for Data-sharing in Practice – which we will now proceed to explore in more depth…*	
	A Framework for Data-sharing in Practice. Facilitator presentation @plenary	
	Present the OCHA-PIM Team Co-led process and outcome for the *Framework*. Explain the background and purpose of the *Framework* (See Facilitator note 8). Provide an (introductory) overview (not going into details) of the 5 elements of the *Framework*. Emphasize links to the existing PIM resources and reference points, and explain that in this module we will be dwelling on the 1st and 5th elements in more detail (you may note that all of the elements are explained in the Module learning sheet): 1. Trust Statement - An articulation of the elements of a trustworthy and overall better data sharing environment, either within an organization or between organizations (**Will be covered in detail next**). 2. Shared definitions and concepts: - PIM Principles and shared definitions e.g. terminologies and PIM Matrix. 3. Core Competencies: - The 32 PIM Core Competencies - generally not present in one person; but should be present when IM and protection colleagues working together. 4. Shared process for the design, handling, sharing and use of data: - The PIM Process. 5. Joint Benefit and Risk Assessment - Offers an approach for undertaking a joint benefit and risk assessment (operating within the shared minimum principles, competencies, process) (**Will be covered in detail next**).	PPT,p.13-14
	The Trust Statement. Facilitator presentation @plenary	
	Proceed to show the 'Trust Statement' (See Facilitator note 9), and explain: - *This is the basis on which the other elements rest, since it sets out to create an environment of minimum shared concepts, competencies, principles and process, from which a shared assessment of benefit and risk may take place between two or more parties for a given data sharing scenario.* Call for reflection on each of the paragraphs, ensuring the following points are covered: - Sharing in a "*responsible, safe, and purposeful manner*" – This ties to the PIM Principles and relates to the objective of PIM to *"…provide quality data and information on people in displacement in a safe, reliable and meaningful way*" and the "defined purpose" PIM principle. As such sharing in a "*responsible, safe, and purposeful manner*" should be understood to be a prerequisite for PIM. - *"We understand the risks of sharing and **not** sharing"* – Why is the risk of not sharing explicitly referenced? We may often decide to not share in order to avoid risks, but we should be aware that not sharing entails risks as well. By not sharing essential data and information, the persons whose protection this relates to can be placed at risk,	PPT,p.15

	humanitarian actors may be duplicating efforts to collect data and information on the same issues etc. - *"we will help create an enabling environment that enhances coordination and collaboration"*- Why is a *Framework* needed for this, can it not simply be enough to that we set out to share in a "*responsible, safe, and purposeful manner"* by not sharing without prior 'benefit and risk assessment'? - *Highlight that the thinking behind the trust statement is that if there has been a break in trust established under the Framework, then it is up to the stakeholders involved to understand why and the implications of the Framework among them.* - *The Framework may need to be renegotiated based on whatever those terms are or may no longer exist between the parties.* Call for reflection by asking participants – 'why would we need a 'Trust Statement' – when there already Data Transfer Agreements out there?' (). Ensure that conclusion is drawn that: - *The two are not mutually exclusive.* - *The Trust Statement creates an enabling environment, whereas a DTA only relates to a specific agreement for directly involved parties.* Point out that the Trust Statement text is also available in the Module Learning Sheet for future reference.	
	'Joint Benefit-Risk Assessment'. Facilitator presentation @plenary	
	Explain the concept of the 'Joint Benefit and Risk Assessment' of the *Framework* (Facilitator note 10), making the below points: ● *It offers an approach for undertaking **a joint benefit and risk assessment** (**operating within the shared minimum principles, competencies, process**);* ● *"Benefits" refer to the benefits of sharing, i.e. those things we define and jointly agree we can do with the shared data and information, as defined and jointly agreed to;* ● *The objective is:* ▪ *to ensure that the benefits and risks of data sharing have been systematically and deliberately assessed prior to sharing, and;* ▪ *that actions have been identified to maximize benefits and minimize risks.* ● *It consists of 4 steps (assess information landscape, design IM systems, implement IM systems, evaluate impact) and associated questions, which follow the overall PIM Process.* ● *The listed questions and actions are indicative and descriptive rather than prescriptive.* ● *It can be undertaken by two or more partners/counterparts – who would then decide to proceed or not (with the shared) based on a shared analysis of benefits and risks.* ● *Parties do not need to conduct the entire process together, prior to sharing (some of these shared elements are a given, based on a voluntary participation to operate within an environment of trust).* Introduce the (overall) questions of the 'Joint Benefit and Risk Assessment' (do not go into detail on the guidance for each. As relevant relate the questions of the 'Joint Benefit and risk Assessment' to the points made by participants (based on recommendations made during the previous activities throughout this module – refer to the flipchart notes). Ask participants to recall their own experiences with data sharing (as per the results of the pre-training survey) and the dilemma which they discussed earlier in the module. Ask to reflect on whether the outcome of their discussion. Ask them if a Joint Benefit Risk	PPT,p.16-18

	Assessment could have served to enable safe, responsible and purposeful sharing in the case which they reviewed. Invite participants to share their individual reflections in plenary.	Flipcharts (stands+ paper)
	Conclusion. Facilitator presentation @plenary	
	Summarize topics which emerged during the module in relation to the module key messages, review module objectives and answer any outstanding questions. Remind participants to save their notes on the suggestions to take forward to promote safe, responsible, and purposeful sharing of data in own context, and to present these to relevant stakeholders in their own contexts post-training. Recap the module learning objectives and learning outcomes. Refer to the fact that the Module learning sheet includes relevant links (e.g. the *Framework*). Project "Moment of Zen" video (2.5 min, Sesame Street 'Sharing', message: (Safe, responsible and purposeful) sharing is win-win): https://www.youtube.com/watch?v=YnD1t2O8vAE Distribute module feedback form (one per participant) and collect the filled in version from participants before module closure.	PPT,p.19-20 Projector, speakers and internet Module feedback form (Annex 5.2.c)

Facilitator note 1) Recommended resources

ESSENTIAL READING

International Committee of the Red Cross (2013, 3rd edition in 2018, forthcoming): Professional Standards for Protection Work, Chapter 6 "Managing Data and Information for Protection Outcomes", available at: https://www.icrc.org/en/publication/0999-professional-standards-protection-work-carried-out-humanitarian-and-human-rights

Office for the Coordination of Humanitarian Affairs (OCHA) & PIM (2017): A Framework for Data Sharing in Practice: Summary Report, Part I, available at: http://pim.guide/wp-content/uploads/2017/09/OCHA_PIM_Framework-for-Data-Sharing-in-Practice_Part-I.pdf

Office for the Coordination of Humanitarian Affairs (OCHA) & PIM (2018): A Framework for Data Sharing in Practice: Summary Report, Part II, available at: http://pim.guide/guidance-and-products/ocha-pim-a-framework-for-data-sharing-in-practice-summary-report-part-ii/

PIM Principles in Action document, available at: http://pim.guide/wp-content/uploads/2017/01/PIM-Principles-in-Action_-2017.pdf

PIM: A Framework for Data Sharing in Practice (2018) available here: http://pim.guide/wp-content/uploads/2018/05/Framework-for-Data-Sharing-in-Practice.pdf

WEBSITES

PIM Website (www.pim.guide)

PIM RESOURCES

PIM Core Competencies, available at: http://pim.guide/wp-content/uploads/2017/01/PIM-Core-Competencies-Framework_v4.pdf

PIM Principles, available at: http://pim.guide/wp-content/uploads/2018/04/PIM-Principles_one-pager_2018-1-1.pdf

PIM Process, available at: http://pim.guide/guidance-and-products/product/pim-process/

PIM Matrix, available at: http://pim.guide/guidance-and-products/product/pim-matrix-cover-page/

PIM Common Terminology (2018 ed.), available at: http://pim.guide/wp-content/uploads/2018/04/Protection-Information-Management-Terminology_Revised-Edition-April-2018.pdf

PIM Working Group Meeting #2 (Dec 2015): Meeting Outcome document available at: http://pim.guide/wp-content/uploads/2016/10/Protection-Information-Management-Working-Meeting-Outcome-Document_Dec-2015.pdf

PIM Working Group Meeting #3 (Sep 2016): Meeting Outcome document available at: http://pim.guide/wp-content/uploads/2017/01/Protection-Information-Management-Working-Meeting-Outcome-Document_September-2016.pdf

OTHER RESOURCES

Harvard Humanitarian Initiative (2017), Signal Code: A Human-rights based approach to information during crisis, available at: https://hhi.harvard.edu/publications/signal-code-human-rights-approach-information-during-crisis

International Committee of the Red Cross (2013, 3rd edition in 2018, forthcoming): Professional Standards for Protection Work, Chapter 6 "Managing Data and Information for Protection Outcomes", available at: https://www.icrc.org/en/publication/0999-professional-standards-protection-work-carried-out-humanitarian-and-human-rights

International Committee of the Red Cross (ICRC) (2016): Rules on Personal Data Protection, available at: https://www.icrc.org/en/publication/4261-icrc-rules-on-personal-data-protection

International Committee of the Red Cross and Brussels Privacy Hub (2017): Handbook on Data Protection in Humanitarian Action, available at: https://shop.icrc.org/handbook-on-data-protection-in-humanitarian-action.html?___store=default

Oxfam (2017): Responsible Data Management training pack, available at: https://policy-practice.oxfam.org.uk/publications/responsible-data-management-training-pack-620235

United Nations High Commissioner for Refugees (UNHCR) (2015): Policy on the Protection of Personal Data of Persons of Concern to UNHCR, available at: http://www.refworld.org/docid/55643c1d4.html

Facilitator note 2) Data and information typologies

a. Data and information

'Data' means a collection of facts, such as numbers, measurements, or observations, whereas 'information' means facts or details about a subject.

(Source: PIM (2016): Commonly used Protection Information Management Terminology, available at: http://pim.guide/wp-content/uploads/2017/01/Commonly-used-Protection-Information-Management-Terminology_June-16.pdf)

b. Protection data and information

Data and information pertaining to protection risks/issues and situation of specific individuals/groups.
We can largely distinguish between:

- Personal Identifiable Information (PII): which can lead to identification of an individual.
- Community identifiable information (CII): which can lead to identification of a community.
- Demographically identifiable information (DII): which can lead to identification of specific demographic entity.

(Source: PIM (2016): Commonly used Protection Information Management Terminology, available at: http://pim.guide/wp-content/uploads/2017/01/Commonly-used-Protection-Information-Management-Terminology_June-16.pdf)

What is personally identifiable data vs. non-personally identifiable data?

The current definitions of personally and non-personally identifiable data continue to be challenged by modern technology. Because we are dealing with human data, it may all carry the risk of being personally identifiable. It is recommended to instead focus on how to prevent harmful use and how to assess risk through the operationalization of a shared risk and benefit assessment. Doing so can clarify the actions needed to assess or prevent risk, based on a series of steps. The shared analysis of the risks and benefits for a particular data sharing process would then be the component of this process that is shared.

(Source: PIM: A Framework for Data Sharing in Practice (2018) available here: http://pim.guide/wp-content/uploads/2018/05/Framework-for-Data-Sharing-in-Practice.pdf)

c. Sensitive protection data and information

Sensitive protection data and information is data or information whose disclosure or unauthorized access is likely to cause:

- harm (such as sanctions, discrimination, repression or stigma) to any person, including the source of the information or other identifiable persons or groups; or
- a negative impact on an organization's capacity to carry out its activities, including due to reputational damage.

Sensitivity of data is defined in relation to the particular context, and the level of aggregation and may change over time. Therefore, the same data may not have the same level of sensitivity in different contexts. Protection data and information that does not contain personal data may nevertheless be sensitive. It may relate to communities and other groups, to anonymous individuals, or to specific events or issues. In armed conflicts and other situations of violence, various aspects relating to the humanitarian, human rights, political or security situation may exacerbate the risks to people.

Likewise, aggregated or pseudonymized data may still be sensitive. Individuals or groups may still be identifiable, especially depending on the location and sample size, and thus may be exposed to harm if data about them is disclosed. It is therefore not possible to propose a definitive list of what types of data or information constitute sensitive information. However, some key types of information may belong to this category, including information about the nature of violations affecting specific individuals or groups, details about victims and witnesses, the affiliation of perpetrators, operational details related to military operations or security, etc.

Recognizing that the privacy, security and integrity of individuals or groups may be put at risk even if no personal data is collected and processed, protection actors as a matter of best practice apply the standards derived from the principles of data protection to sensitive data and information used for protection purposes, to the extent that it is necessary given the particular sensitivity of the data.

(Sources: International Committee of the Red Cross (2018, 3rd edition forthcoming): Professional Standards for Protection Work, Chapter 6 "Managing Data and Information for Protection Outcomes").

d. Personal data

Personal data, also known as personally identifiable information (PII), is data relating to an identified individual or to a person that can be identified from that data, from other information or by means reasonably likely to be used related to that data. This could include, for instance, an identifier such as a name, an identification number, location data, audio-visual material, or an online identifier. Personal data also include: country of asylum, individual registration number, occupation, status, religion and ethnicity. And it

includes biometric data such as a photograph, fingerprint, facial or iris image, as well as any expression of opinion about the individual, such as an assessment of their legal status and/or specific needs.
(Source: Office for the Coordination of Humanitarian Affairs (OCHA) & PIM (2018): A Framework for Data Sharing in Practice, available at: http://pim.guide/wp-content/uploads/2018/05/Framework-for-Data-Sharing-in-Practice.pdf).

e. Sensitive personal data

Sensitive personal data are personal data that, if disclosed, are likely to result in harm (such as discrimination) for the individual concerned. As a result, many of the international instruments on data protection mentioned in this chapter include stricter rules for the processing of sensitive personal data. Given the specific situations in which protection actors work, and the possibility that some data could give rise to discrimination, setting out a definitive list of categories of sensitive personal data in protection contexts is not meaningful. Sensitivity of data and appropriate safeguards (e.g. technical and organizational security measures) will be context-dependent and may change over time within a given context; therefore, they need to be considered on a case-by-case basis. Data relating to health, race or ethnicity, religious/political/armed group affiliation, and genetic and biometric data are considered to be sensitive personal data at all times. The nature of violations and abuses affecting specific individuals or groups, and the identity of perpetrators and witnesses, also fall into this category. All sensitive personal data require additional protection even though different types of data falling within the scope of sensitive data (e.g. different types of biometric data) may present different levels of sensitivity.
(Sources: International Committee of the Red Cross (2018, 3rd edition forthcoming): Professional Standards for Protection Work, Chapter 6 "Managing Data and Information for Protection Outcomes").

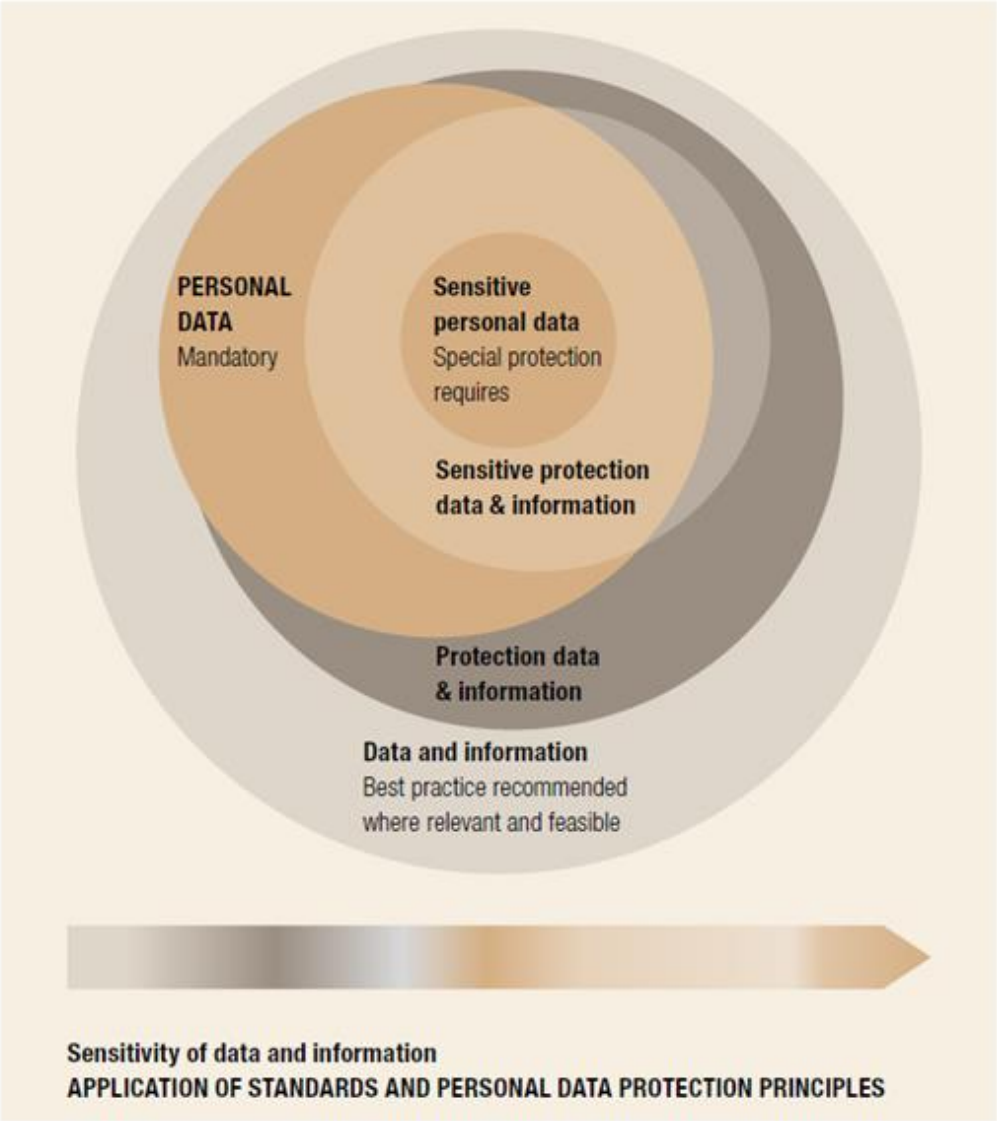
f. Confidential data (pre-labelled categories)

Confidential data is data for which will not be disclosed or otherwise made available to unauthorized persons or entities in ways that are inconsistent with the understanding of the original disclosure or without prior consent. There is an obligation to exercise utmost discretion with regard to all matters. Information known shall not be communicated to any Government, entity, person or any other source, nor made public.' (UN Staff Rules and Regulations (e.g. Regulation 1.2.g.) Information received from sources and clients will only be used and/or shared for specific purposes only when the person in question has provided specific and informed concern to do so. (OHCHR Code of Conduct). Even if consent for the use of information is given, the potential implications of that action for the safety of the person providing the information and of other people involved in the situation (e.g., the family of witnesses) must be assessed. If there is a risk of endangering any of them, the information should not be disclosed or in a manner that removes the risk. The safety of victims, witnesses and other cooperating persons must be a paramount concern; confidentiality as a measure to protect their safety should therefore take precedence over other considerations.
(Source: Office of the High Commissioner for Human Rights (2001): Manual on Human Rights Monitoring, Chapter 2, p. 6, available at: http://www.ohchr.org/Documents/Publications/Chapter02-MHRM.pdf).

Facilitator note 3) Diagram: Sensitivity of data and information

The below diagram from ICRC illustrates the relationships between types of Data and Information in relation to sensitivity levels and required measures for protection.

Diagram: Relationships between types of data and information



(Source: International Committee of the Red Cross (2018, 3rd edition): Professional Standards for Protection Work, Chapter 6 "Managing Data and Information for Protection Outcomes", available at: https://www.icrc.org/en/publication/0999-professional-standards-protection-work-carried-out-humanitarian-and-human-rights)

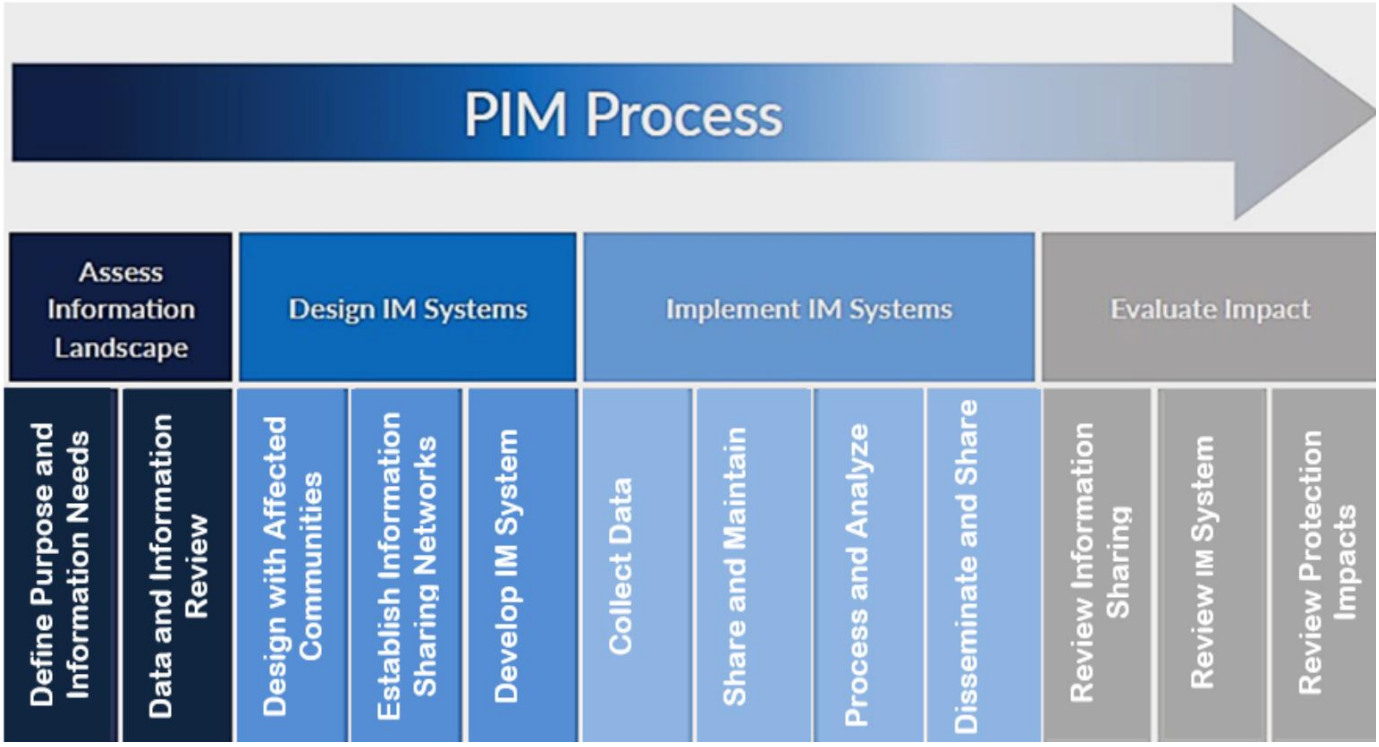
Facilitator note 4) PIM Process

The PIM Process provides guidance on steps to be undertaken when developing, implementing or renewing a protection information management response / set of activities. The PIM Process is an organic and potentially an iterative process. While the four higher-level steps of the PIM Process — Assess Information Landscape, Design IM Systems, Implement IM Systems, Evaluate Impact — are prescriptive and should be followed in this sequence, the sub-steps, however, falling under these may be followed in a prescriptive or a non-prescriptive manner, i.e., they do not necessarily require step-by-step implementation/adherence.

Working with and using the PIM **Process for a given data sharing arrangement or scenario, is** open to two or more parties both inside and outside the humanitarian community (e.g. affected populations, development and peacebuilding actors, academics, private sector, media), based on the needs of a given data sharing situation.

Recognition of a defined process allows for a structured approach and clear communication and understanding regarding what work is being done, while providing a minimum structure from which to assess a request or a given response.

The intent is not to have everyone adapt their entire information management process, but rather for them to share a clearly defined minimum process and approach to support good practice. The shared process is



further reflected in the key **questions** to ask and **actions** to take when undertaking a joint benefit and risk assessment for a given data sharing arrangement.

(Source: PIM Working Meeting, September 2016, available at: http://pim.guide/wp-content/uploads/2017/01/Protection-Information-Management-Working-Meeting-Outcome-Document_September-2016.pdf

Facilitator note 5) Three Spheres of Data Sharing Challenges

The examples below are illustrative (not comprehensive), and aim to facilitate the discussion. Participants are not expected to list all the items, but rather to understand how their challenges can be organized along these three spheres.

1. Practical & Procedural

- Data protection and security concerns (e.g. lack of ability to identify and implement appropriate data security measures).
- Lack of clear SOPs, reducing predictability (i.e., data holders do not know how to use and share it, when, and why).
- Difficulties in ensuring the quality, validity, and integrity of meta-data.
- Technical issues with hardware, software and tools.
- Inappropriate data sharing and data breaches.
- Lack of standardized formats and processes.
- Multiplicity of platforms.
- Remote environment reduces ability to share (when there is willingness).
- Weak Accountability to Affected Populations (AAP) or communication within(in) communities (e.g., about the data that has been collected and will be shared).

2. Institutional & Structural

- Working with legal and institutional mandates, and country-specific policies.
- Working with existing data protection SOPs and policies (and lack of enforcement for use of outdated SOPs).
- Engaging all clusters to share relevant data.
- Lack of awareness of data-sharing protocols.
- Collaboration with actors outside humanitarian community, e.g. peacekeeping missions and development actors.

3. Mind-set and Trust

- Feeling that humanitarian actors do not want to share.
- Competition between humanitarian actors (information = power & influence).
- Different personal and professional pressures, incentives and sanctions – both to share and to not share.
- Different assumptions and world views (e.g., about what is necessary and appropriate…).

Facilitator note 6) Data Protection Impact Assessment (DPIA)

DPIA is a tool and process for assessing the protection impacts on data subjects in processing their personal data and for identifying remedial actions as necessary in order to avoid or minimize such impacts. It helps organizations identify, assess and mitigate or minimize privacy risks with data processing activities. A DPIA should be conducted where data processing is likely to result in a high risk to the rights and freedoms of natural persons.

(Source: ICRC Handbook on Data Protection in Humanitarian Action (2017) contains recommendations for who to conduct DPIAs for specific data types in Chapter 6, p.64-67, available at: https://shop.icrc.org/handbook-on-data-protection-in-humanitarian-action.html?___store=default)

Facilitator note 7) Data Transfer Agreement (DTA)

A DTA states the terms and conditions around sharing and use of personal data, including which data components are to be shared, the mode of transfer, how the data may be used, data security measures and other related issues. As per the UNHCR Policy on the Protection of Personal Data of Persons of Concern to UNHCR "*Data transfer agreements should, inter alia: (i) address the purpose(s) for data transfer, specific data elements to be transferred as well as data protection and data security measures to be put in place; (ii) require the third party to undertake that its data protection and data security measures are in compliance with this Policy; and (iii) stipulate consultation, supervision, accountability and review mechanisms for the oversight of the transfer for the life of the agreement*".

(Source: UNHCR (2015) Policy on the Protection of Personal Data of Persons of Concern to UNHCR: http://www.refworld.org/pdfid/55643c1d4.pdf)

Facilitator note 8) A Framework for Data Sharing in Practice

Data is a clear prerequisite for improved humanitarian response. Yet the push for quality data and evidence has not been matched by a similar rise in the sharing and use of data collected. Safe and responsible sharing is challenging. In the present time, we have more ways to collect, store, share, transmit, analyse and publish data than ever before. There is currently no common framework for whether, how, why, and when data is shared in support of humanitarian action and protection response. The absence of a common framework can result in several adverse outcomes, including less or no sharing, irresponsible sharing, or confusion among partners about what can or should be shared. Each of these can result in a loss of the knowledge and evidence needed for decision-making and response, both internally and with operational stakeholders and partners.

The PIM Initiative is setting out to explore ways for collectively facilitating & advancing the safe, responsible & purposeful sharing of data, information and analysis for stronger humanitarian response & protection outcomes.

In 2017, PIM and OCHA initiated a process to Identify elements of a *Framework* that may set practical minimums to facilitate the safe, responsible and purposeful sharing of data, information and analysis for stronger humanitarian response and protection outcomes. The *Framework* is not about absolutes but rather about offering practical minimums based on good practice.

The *Framework* starts by setting out a common 'trust statement'. Above all, this establishes a commitment to work within the *Framework*, in support of responsible data sharing.

The *Framework* articulates a minimum level for shared principles and process open to actors both inside and outside the humanitarian community (e.g. affected populations, development and peacebuilding actors, academics, private sector, media), based on the needs of a given data sharing situation. For any individual data sharing scenario, two or more colleagues would come together and undertake a joint assessment based on their context and situation.

The *Framework* then defines in concrete terms how to undertake a joint benefit and risk assessment in an environment of trust. Such an assessment explores the benefits and risks of sharing specific data or information within a given context, after which stakeholders can make an informed decision on if and how to proceed with the sharing arrangement.

If there has been a violation of the *Framework,* it is up to the stakeholders involved to understand why the violation took place and then to decide whether to continue to share, or any additional ramifications. If the

initial trust is broken, the *Framework* would need to be renegotiated, or the *Framework* may no longer exist between the parties

If colleagues are not operating in an environment of trust, it becomes more difficult to assess the risks and benefits of data sharing for any given situation.

(Source: PIM (2018): A Framework for Data Sharing in Practice, available here: http://pim.guide/wp-content/uploads/2018/05/Framework-for-Data-Sharing-in-Practice.pdf

Facilitator note 9) The Framework's Trust Statement

The Trust Statement indicates a commitment to act in accordance with the *Framework,* signalling that 'I as a person' and/or 'we as an organisation' will behave in accordance to the trust statement and the minimum standard outlined in the overall *Framework.*

The objective of the trust statement is to articulate the elements of a trustworthy and overall better data sharing environment, either within an organization or between organizations. For example, if you are in the process of negotiating a data sharing agreement you may still need to refer to the *Framework* for steps that may need to be completed or considered in that process and mutually agreed upon.

The trust statement is about establishing an environment of trust and the ways in which trust can be created, maintained, and enhanced requires working in a spirit and practice of trust, with a shared minimum approach to ensure good practice. This approach is outlined in the elements of the *Framework* below.

The Trust Statement will be a statement which two parties will agree to as an indication of their commitment to the *Framework* when sharing data. The statement may also extend to donors, who have the responsibility and leverage to enable data sharing and cooperation among stakeholders.

Text of the Trust Statement:

> *We recognize the benefits of sharing data in a responsible, safe, and purposeful manner to improve responses that promote safety, dignity, and the rights and capacities of affected populations.*
>
> *We understand the risks of sharing and not sharing, and we commit to sharing and receiving data, information according to the humanitarian principles and in line with protection and information management [PIM] principles and respective organizational policies on the same.*
>
> *Equipped with the Framework for Data Sharing in Practice, we will help create an enabling environment that enhances coordination and collaboration within and beyond the humanitarian community for data sharing.*

Facilitator note 10) Benefit Risk Assessment – guiding questions

The objective of the joint benefit and risk assessment is to ensure that the benefits and risks of data sharing have been systematically and deliberately assessed prior to sharing, and that actions have been identified to maximize benefits and minimize risks. This is especially important to determine the purpose of the data and the purpose of the data sharing, understanding trust, and understanding characteristics of the data and reasons to share in any given situation.

The element of a/ the data process ***that is shared /done jointly*** is the benefit and risk assessment. It is important to jointly be able to identify the various sides of the benefit and risk equation, and to put these

together for a more complete overview. In turn, this broader understanding can inform the context and temporal conditions around the specific uses of the data sharing, including informing the means, modalities, and frequency of the specific data sharing arrangement.

The Framework outlines key **questions** to ask and key **actions** to take along with supporting guidance, when undertaking a benefit and risk assessment for a given data sharing arrangement.

For ease of reference in conjunction with module delivery, the questions are listed below (for full details of also key actions and guidance you are advised to see the Framework):

Step 1: Assess Information Landscape

Q1. Does the purpose for data sharing benefit the safety and dignity of affected populations? Is it critical? What are the potential negative impacts or harms of not sharing the data?

Q2. Can the data collecting and receiving parties demonstrate the required core competencies and the respect for the minimum Principles and Process?

Step 2: Data and Information Review

Q1. What do we need to know? Does this data need to be shared or is it already public? Have you done a secondary data review?

Q2. Have you clearly defined what is 'sensitive' data in your specific context? What is the level of detail and the type of data to be shared? Consider personal and/or sensitive data, vs. trends, statistics and other analysis? How have you considered context, time, the impact on the individual or community to whom the data belongs and the impact on staff security?

Q3. If personal data is collected/shared, was informed consent obtained (as per international standards), for the intended purpose?

Q4. How can we maximize the benefits of data (collection) and sharing within and beyond the humanitarian sector?

Step 3: Implement IM [Sharing] Systems

Q1. Have new benefits or risks emerged in the implementation stage? If so, have the prevention and mitigation actions identified in Step 2 (under 'Data and Info Review') been successfully implemented?

Q2. Do the users of the data or information demonstrate an understanding of relevant standards (e.g. PIM principles), procedures, and policies?

Step 4: Evaluate Impact [of Sharing]

Q1. Have you been able to evaluate the data sharing arrangement?

Q2. What were the impacts of the data sharing?

Q3. Was information shared with the affected populations as planned? What was the feedback and how was it considered regarding their use of and access to the information?

Q7. Was the identified information shared as planned? Was it more/less sufficient for the purpose?

ANNEXES TO MODULE 5.2

Annex 5.2.a) "Benefit versus Risk dilemma" cards
Module: 5.2 Data sharing
Instructions for production and delivery: Print and cut the cards (number of cards should match the number of participants). Participants will discuss the dilemmas on the cards in pairs.
Available at: https://docs.google.com/document/d/1vsO___Yfi9grQNNQ_IS7dkgvmLbR--dLpIF1zAnuD6Y/edit?usp=sharing

Annex 5.2.b) Module learning sheet: Data Sharing
Part of module: 5.2 Data Sharing
Instructions for production and use: The Module learning sheet should be printed one for each participant and serve as learning reference point for the participants throughout and after the module. It contains structured space for note taking on key concepts introduced, contains reference tools, definitions and a list of recommended resources for further learning. One per participant.
Print out available: https://docs.google.com/document/d/14aX-TWSM2kM2kSpGZMxHg-HYvXuKdZ08gXEzN79928k/edit?usp=sharing

Annex 5.2.c) Feedback form for 5.2 Data Sharing
Part of module: 5.2 Data Sharing
Instructions for production and use: The standardized and anonymous feedback form should be handed to participants after completion of the training module (one for each) for immediate completion and return to the facilitator, in order be used by the facilitator to evaluate the extent to which the module learning objectives have been met through realization of the module learning outcomes. The form will take 3-5 minutes to complete.
Print out available: https://docs.google.com/document/d/1-nETZlU-MGFtWm-FVCnYx_oFmpwhkvGDsoXBAWjXAVs/edit?usp=sharing

Annex 5.2.d) Power point presentation
Part of module: 5.2 Data Sharing
Instructions for production and use: This power point presentation may serve as visual reference during delivery of this module. Please note that facilitators are discouraged from rely sole on the power point presentation as visual reference during module delivery, as this is not compatible with the participatory design of the PIM training modules.
Available at:
https://www.dropbox.com/s/wymtm9ffngv1wlg/PPT_Packge%205_Module%205.2_Data%20Sharing.pptx?dl=0