Recommendations on the Outcome of the Protection Incident Monitoring and Case Management Workshop

24-25 May, 2011
CICG, Geneva

Introduction

This paper outlines the challenges and recommended good practices with regard to protection incident monitoring and case management systems. These systems are used by multiple organizations in humanitarian operations in several countries. Specifically, the recommended good practices captured here are addressed to the members of the Global Protection Cluster as the paper looks at potential linkages and coordination opportunities between agencies and their respective systems in enhancing protection monitoring and case management.

The paper is based on discussions that were held at the interagency Protection Incident Monitoring and Case Management Workshop organized by UNHCR and hosted by the Global Protection Cluster in Geneva on the 24-25 May 2011.

For the purposes of this paper, 'Protection incident monitoring systems' are defined as tools and procedures applied in a systematic way to identify and record violations of human rights, otherwise "protection incidents" and to chart related trends and changes. . 'Case management' and 'data management' have been differentiated, with the former referring to efforts to manage information in order to provide targeted services to individuals, and the latter referring to the application of systems to produce statistics for strategic and operational planning, advocacy and multi-level interventions from the global to the community based. The Good Practices and Challenges sections of this paper are organised to respect these distinctions. The term "survivor" is used to refer specifically to those individuals who have survived protection incidents and who will receive individual-level protection case management services and assistance; the term "victims" is used more generally to describe any persons victimized through human rights violations which occur during protection incidents. Victims can include survivors as well as those who have died.

Background, Protection Incident Monitoring Workshop

This two-day inter-agency workshop was convened in Geneva on 24-25 May, 2011 to allow agencies to familiarize themselves with existing protection incident monitoring and case management systems in the inter-agency space and to demonstrate their own systems to other agencies. It also sought to provoke discussion and analysis of these systems and to document good practices and potential areas of synergy between different organizations' systems. Both general systems and specialized ones (e.g. GBV, Child Protection) were analyzed and discussed during the workshop, which had three specific objectives:

1. To analyze existing protection incident monitoring systems, including both specialized ones (GBV, Child protection) and general ones to document good and poor practice, as well as areas of potential synergy.
2. To coordinate, where possible, linkages between protection monitoring systems and MRM (Security Council Resolutions 1612, 1960, etc.).
3. To strategize on a way forward for improving coordination of protection incident monitoring and case management systems in humanitarian operations.

The workshop was attended by 38 participants from a variety of organizations, including UNICEF, UNFPA, IRC, UNHCR, OHCHR, NRC, UN Women, ProCap, OCHA, ICRC and UN ACTION. The following eight different systems were presented during the two days: UNICEF's Monitoring and Reporting Mechanism database (MRM), the Interagency Child Protection Database (IA CP IMS), UNHCR's proGres, ICRC's Prot5, the interagency Gender Based Violence Information Management System (GBVIMS), OHCHR's Human Rights Case Database (HRDB) and UNHCR's Promis.

The workshop's outputs include:

1. a comprehensive inventory[1] of existing protection incident case management and monitoring systems, and
2. this document, which provides a summary of recommended good practices and challenges in the operation of protection incident monitoring and case management systems.

Summary of Proceedings

1. Independent Systems Working Better Together: Establishing or coordinating referral mechanisms between case management systems (Karin Wachter, IRC)

The overall goal of this session was to explore whether or not the various protection incident monitoring and case management systems support referrals of survivors between service providers, and if so, how.

Outcome: It was found that when systems did have a referral pathway tracking mechanism, efforts had been made to suggest possible improvements in service delivery, statistical reporting and / or protecting data confidentiality. Challenges and good practices were discussed and different models of referral mechanisms were shared. Participants highlighted specific information management challenges with tracking referrals but the discussion understandably focused primarily on the long-standing challenges with establishing effective referral systems. These challenges included: pre-emptive referrals and data-sharing between service providers and a coordinating agency (therefore, not based on survivor choice or specific need); geographical distance between service providers; difficulties with following up on referrals to continue client advocacy or to ensure

[1] Note: a copy of the inventory can be requested by contacting the Global Protection Cluster Secretariat.

the expected services were rendered; sharing the right information with the community to encourage help-seeking behaviors to the most relevant and appropriate service provider.

2. Independent Systems Working Better Together: Statistical harmony between system reporting outputs (Shelley Gornall, UNHCR)

The level of statistical harmony between organizations' systems will directly affect the quality and extent of protection incident statistics and information available to international actors. This session explored the purposes and challenges of protection incident statistics with specific attention to prevalence, verification processes, incident typologies, double counting and units of measurement.

Statistical analysis can be used for profiling victims and perpetrators as well as trend analysis that can be applied in, strategic and operational planning, prevention programming, advocacy and mutil-level interventions from the global to the community based.

- **Victim profiling**
    - Victim profiling is a statistical analysis of protection incident data that allows humanitarian actors to identify characteristics of persons likely to report particular types of incidents and to take preventative action to protect those who may be targeted or otherwise vulnerable. Victim profiling entails the collection of information about victims for trend analysis, including bio-data as well as other characteristic information such as their activities when the incident occurred. In general, this practice can serve to improve targeted programming and, when combined with perpetrator profiling, may assist service providers in revealing trends with regard to those being targeted and those who are actively reporting protection incidents. However, it is important to remain aware when including this facility in a monitoring system, that the victims' trust and willingness to cooperate may be negatively affected by the level of personal information they are asked to provide. Thus, data security and de-identifying data as a general rule is encouraged. It is also important to highlight that only actionable data should be collected.
- **Perpetrator profiling**
    - Perpetrator profiling is a method of identifying trends based on an analysis of the nature of the violation and the manner in which it was committed by the perpetrator. Perpetrator profiling is not aimed at gathering evidence to the level of detail associated with criminal prosecution, but instead, analyzing trends in protection incidents (e.g. relationship of the alleged perpetrator to the survivor and his / her occupation). This type of information can be of significant value when analyzing trends and linkages, specifically when other evidence is not available. The collection and analysis of such information is encouraged and can be extremely actionable when behavior patterns can be extracted. However, the collection and analysis of such information can be controversial, especially for those providing survivor services. It is encouraged to weigh the pros and cons of collecting such data very carefully and only include the data that does not put the survivor or service provider at risk. In addition, when collecting perpetrator profile data, it should be noted that some information is very difficult to ascertain (e.g. where survivors are asked to indicate whether the perpetrator belonged to a specific armed faction); thus, the

humanitarian community should not put undue pressure on service providers or survivors to provide any information that is difficult for them to provide accurately and/or may put them at risk.

- The discussion highlighted five potential ways of working better together by harmonizing our systems from a statistical standpoint:

1) to focus on the physical act when classifying incidents instead of incorporating victim / perpetrator characteristics within the incident type

When a physical act (e.g. rape, murder, arbitrary detention) is involved in the protection incident, the primary classification of the incident should focus on the physical act, without combining victim and perpetrator characteristics. For example, "gang rape", "incest" and "spousal rape" are all forms of rape; if characteristics of the victim or perpetrator are combined with the classification, then incident types proliferate and statistical meaning is lost. .

2) to harmonize different incident taxonomies between systems into a mega taxonomy at the global/country level

Where feasible at the global or country level, incident taxonomies should be compared and harmonized in order to ensure that the data resulting from different organizations' systems is as compatible as possible. Harmonization might mean that protection organizations agree on a simple set of larger-groups to which specific incident types captured by different humanitarian actors can map.

3) to count using an explicitly defined unit of measurement

The main units of measurement for statistical analysis in all the protection incident systems are:

a) incident

b) victim / survivor

c) violation

One incident may involve multiple victims; one victim may have had multiple human rights violations. In order for protection incident statistics to be meaningful and to reflect the extent and severity of what is being reported, it is important for any system to have explicit criteria to define whatever unit of measurement is being used (e.g. when does one incident end and another incident start?). When different protection incident systems use different units of measurements, the resulting statistics cannot be compared.

4) to prevent double counting

Methods of avoiding double counting through standard operating procedures and more systematic means (de-duplicating data) were discussed. Because of the sensitive nature of protection incident data and the limitations in sharing it, double counting is often a statistical problem that needs to be minimized by multiple strategies.

5) **to systematize the bias in incident classification and incident counting.**

While eliminating bias in counting protection incidents is ideal, it may be difficult to reduce complex incidents to a simple number. However, systematizing the bias – so that different offices and different organizations – are classifying the same types of incidents in exactly the same way, will help with the comparability of data between locations and organizations. Specific techniques for minimizing double-counting are detailed below.

3. Common Incident System: Can we have a common protection incident system in certain situations? (Eddie O'Dwyer, UNHCR)

The idea of a common incident system in certain situations was discussed during this session to explore the need for and feasibility of such cooperation. The group agreed that given the current fragmentation of approaches and systems, no one system could provide the answer in the short to medium term. Rather it was recommended to look for common elements within current systems and to examine how practical linkages and synergies could be developed within Protection Clusters. The discussion also highlighted the need to streamline the protection information management effort, particularly in the early phases of an emergency. Concrete actions included directing our attention to better cross-analysis of data between systems, to develop data sharing methods and protocols, and to define collaboration processes – including cross-referenced SOPs.

4. Security Council Resolution Reporting Compliance and humanitarian space issues (Monika Sandvik-Nylund, UNHCR, Jane Rasmussen, UNHCR)

Ms. Gillian Holmes gave a presentation on proposed Monitoring, Analysis and Reporting Arrangements (MARA) on conflict-related sexual violence, in accordance with Security Council Resolution 1960. The discussion also highlighted the need to further explore the possibility to create synergies between MRM and incident reporting. However, key considerations including service provider protection issues need to be considered. While, Security Council resolution reporting compliance and humanitarian space were discussed extensively, this paper will not attempt to summarize the content of the discussions or take a position given these discussions are continuing in other fora.

Challenges & Good Practices

This section lists a number of key challenges that are faced in operationalizing protection incident monitoring and case management systems. It also highlights corresponding good practices that can be used when designing protection incident systems and managing linkages between different systems. The list of corresponding good practices is not exhaustive, but summarizes some key elements and system features that may increase the ability to provide better protection and services to populations of concern, and potentially enable statistical harmony.

1. Data Systems Supporting Case Management:

- **<u>Informed Consent</u>**
  - **Challenge:**

    Challenges arise due to different levels of informed consent when linking systems and sharing information between the different systems. Some systems examined during the workshop had multiple levels of consent, allowing a survivor to stipulate particular instructions on data usage and sharing, while other systems had "blanket" consent, where it was a situation of giving "all or nothing". Clearly communicating the different forms of consent to survivors so that they have a real understanding of how the data will be used can also pose a challenge.

  - **Good Practice:**

    Every system represented at the workshop included some model of informed consent. Informed consent is a necessary characteristic of protection incident systems; a system without this is sub-standard. Informed consent should be defined clearly on data collection forms, indicating the purpose of the data collection and how the data may be used. How to handle a case where informed consent is not given or is revoked should be detailed in standard operating procedures.

- **<u>Verification Standards</u>**
  - **Challenge:**

    Verification of data – a means of systematically validating the information collected according to established standards – can be a key challenge for a number of reasons. First, there is no standard practice of data verification between organizations. For example, some organizations consider only a direct report from a survivor as verified. Other organizations will accept reports from sources other than survivors and have multiple other levels of verification, including first hand information, direct witness reports and official information from authorities. Because verification standards determine the inclusion in or exclusion of particular information from statistical consolidation, the different standards of verification will create different biases in statistics. For example, a system that only accepts survivor reports and will not accept reports from first-hand witnesses will have lower numbers and different patterns of incident types than one that accepts reports from both. Second, organizations will sometimes have two sets of data, a verified set and an unverified set, which complicates analysis, especially inter-organization analysis. In addition, 'verification' can be construed as requiring a UN staff or UN-endorsed individual to 'check' an organization's records and 'verify' by following up directly with a survivor that the report was valid and true. This interpretation of 'verification' has arisen specifically in the case of Monitoring and Reporting Mechanisms (MRM) established to respond to a UN Security Council resolution (i.e. the protection of children affected by armed conflict, SCR 1612, or conflict-related sexual violence, SCR 1820).

- **Good Practice:**

  Being aware of what other systems' verification criteria are and looking at the metadata around verification can assist in combining one system's statistics with another's. Spot checking verification procedures followed in a randomly selected sample of cases can assist in determining if verification criteria were consistently applied. However consideration should ensure spot checks do not breech the confidentiality of survivors. Where possible, systems that use the same or similar verification criteria will be easier to compare and harmonize. Making notes of the different verification criteria used between systems in statistical analysis reports will assist in explaining differences in outputs between systems.

- **<u>Information Sharing Protocols</u>**
  - **Challenge:**

    Data confidentiality is a challenge when sharing protection incident information. Even when informed consent is given, inappropriate sharing of sensitive data between organizations can compromise the privacy of an individual. Thus, the resistance to share data between organizations is common. The task of establishing MOUs and SOPs that outline sharing protocols is often not prioritized or truncated due to technical discussions. The question of how others will use the data shared is also a point of contention and how to avoid duplicate data continues to be a challenge.

  - **Good Practice:**

    Having documented data sharing protocols enables predictable and safer data sharing. Data sharing protocols dispel confusion and make it explicit on how data may be used between organizations. Anonymization (de-identifying) of data can enable agreement on data sharing protocols. Systems which anonymize protection incident data are more secure because the personally identifiable information is unavailable. Sharing data should not sacrifice the individual's right to privacy. Identifiable data, or case files, should only be shared in the context of a referral for services and with the informed consent of the survivor.

- **<u>Referral Pathway Tracking</u>**
  - **Challenge:**

    Referral pathway tracking enables data systems to systematically follow survivors as they access different services. Key challenges to referral tracking include: weaknesses with quality of referral systems in place and case coordination, making the tracking of such referrals impossible; referrals often stop at mapping the point at which a referral is suggested rather than verifying that a service was indeed received; inadequate agreements in place to govern referrals and how information is shared between service providers; pre-emptive referrals between service providers and having a UN coordinating agency to ensure protection delivery happens.

- **Good Practice:**

  Key elements to a good referral tracking mechanism include:

  - effective systems for case coordination between service providers;
  - up-to-date and accurate standard operating procedures between all service providers;
  - information sharing protocols which facilitate information exchanges between agencies by taking account of their respective systems' functionalities and limits;
  - ongoing provision of training on tracking referrals for service providers along the referral chain;
  - maximum safeguards to protect the confidentiality of information and ensure the safety/security of the survivor;
  - ensuring all referrals are made (and information shared) with the informed consent of the survivor.[2]

  All of the existing systems should review the extent to which they are tracking referrals and how it can be improved. Referrals should not be pre-emptive, thus allowing survivors choice and self determination and a right to privacy.

2. Data Management:

- **<u>Over-Designed Systems</u>**

  - **Challenge:**

    Over-designed systems are those which involve a level of complexity that goes beyond the end users' skills and / or the operational requirements. For example, database administrators may not be available in protection service provider offices. Complicated systems often require resources and knowledge that aren't readily available, thus specialized training, deployments or outsourcing is required.

  - **Good Practice:**

    A shift to simple systems should be explored wherever possible to avoid abandonment of a potentially useful tool, e.g. the use of Excel instead of Access or other relational database management system.

[2] Referrals should not be pre-emptive. The survivor needs to have enough information to choose which services are provided by whom and when services should be accessed, thus allowing survivor choice, self-determination and a right to privacy.

- **Customizing systems**
    - **Challenge:**

      The ability to customize a system to fit specific contextual needs is optimal, but as it is time-consuming up front, it may not be appropriate for emergency situations or time-constrained operations and may lead to incomparable data.

    - **Good Practice:**

      Establish configurable systems that can be locally customized in predictable ways through administrative consoles rather than hard-coding by database developers.

- **Prevalence**
    - **Challenge:**

      None of the systems presented at the workshop claim to produce data on the prevalence of incidents, which is correct. However, there tends to be misperceptions within the humanitarian community regarding the need for prevalence data and what data generated by various systems actually tells us.

    - **Good Practice:**

      Since the statistical output cannot be interpreted as prevalence, organizations must be careful to qualify in their reporting that the statistics only reflect reported cases. Interpretations of protection incident statistics must consider that some cases go unreported.

- **Units of measurement**
    - **Challenge:**

      A core consideration when dealing with units of measurement is to remember statistics cannot be aggregated between systems if different units of measurement are used. For example, some systems count victims, while others count incidents, and still others count violations.[3] Just as one cannot add kilometers and kilograms together, one cannot add statistics that use different units of measurement together. In addition, different standards for defining a particular unit of measurement (e.g. what is an "incident"?) will also produce conflicting statistical results.

[3] Note: Victims, incidents and violations are the three major units of measurements used for protection incident statistics with violations referring to infractions, victims referring to individuals and incidents representing events. For example, in the Gender Based Violence Information Management System (GBVIMS), an incident is defined as something that happens to one person on one day by the same perpetrator(s).

- **Good Practice:**

  Successful practice suggests there needs to be a definition for all three units of measurement. Analyzing systems and trends is possible, but it cannot give a definitive measure by default (e.g. in places where we don't have access or the whole context). Thus bias will naturally be present; hence the need arises to ensure qualitative data by defining the units of measurement used to systematize the bias.[4]

  Using the most atomic unit of measurement can assist in harmonizing statistics. The main units for protection incident statistics are violation, victim and incident with violation being the smallest[5] unit of measurement. Units need to be able to reflect the magnitude and severity of the reported incidents (where most of the reports are coming from). A majority of the systems at the workshop were based on using the victim as unit of measurement.

- **Incident typologies**

  - **Challenge:**

    The challenge with incident typologies is when different systems use different incident types or categories with varying levels of subjectivity. Incidents may be classified differently between individual humanitarian organizations, police or government actors, resulting in an inability to aggregate or cross-analyze statistics from multiple systems. For example, national criminal codes do not always align with international human rights violation categories. Also, flawed typologies / taxonomies with overlapping classifications result in arbitrary statistics from within a single system. The proliferation of incident types is a common problem and will also hinder trend analysis. If types are too precise, there is a reduction in anonymity of the data.

  - **Good Practice:**

    Avoid combining characteristics of a victim or perpetrator in an incident type as it may lead to a proliferation of incident types.[6] A good example of how these combining characteristics can be avoided can be seen in the classification tool developed for the Gender Based Violence Information Management System (GBVIMS).

[4] Note: it can be difficult to systematize violations, making them sometimes hard to analyze. Alternatively, incidents are much easier to systematize.

[5] Note: by smallest, we mean systems that count violations will have the highest numbers.

[6] For example, rape by many perpetrators = gang rape, rape by a parent or sibling = incest, rape by a spouse = domestic violence.

- **<u>Double counting:</u>**
    - **Challenge:**

      The risk of counting the same case multiple times when combining statistical data from multiple organizations or systems is a challenge. Sensitivity of protection data exacerbates this, as not enough data is shared to de-duplicate a central data repository. Double counting is especially likely when geographic areas of systems overlap or when one survivor may seek services from multiple service providers who consolidate statistical data together (e.g. a survivor seeks services from a medical doctor and a psycho-social counsellor who both report the case, resulting in double-counting).

    - **Good Practice:**

      The risk of double counting may be minimized by:

        - dividing up and monitoring territory by geography without overlaps if possible;
        - sharing anonymized data with a central repository to de-duplicate the data or to estimate the amount of possible duplication (training may be required);
        - showing a unique symbol or logo for the survivor to identify if they have already reported the incident within a particular system.

- **<u>Technological Enhancement of Data Security – encryption, tiered access, etc.</u>**
    - **Challenge:**

      Many systems are using encryption, tiered access and log-in security measures, but there should be more attention to ensure security.

    - **Good Practice:**

      Encrypting individual records allows for the electronic transfer of files from one database to another without the possibility of unauthorized interception. Providing safeguard measures (flags/warnings, data audit trails) when users attempt to export/transfer confidential information also prevents unauthorized data sharing and a means of tracing the source of data leaks. Tiered access, in which a user's visibility of the data is determined by their level of responsibility, prevents the over-sharing of information. Having a secure location for the data repository (e.g. in Geneva) may also protect data, but limitations in internet connectivity may not always permit this.

Conclusion

Data management systems should be informed by the best practices currently available. Most pressing is the issue regarding discord in the various protection incident types being used, developed and introduced. In order for protection incident types to be harmonized between systems, an interagency project would need to be initiated which analyzes and cross-maps the various standard definitions used for incident typologies. Given the complexity of this task and the hesitation of organizations to change their incident taxonomies, such goals might be easier to attain in smaller systems at the local level than to attempt harmonization at the global level. For this reason, it is recommended to pilot concrete attempts at such harmonization within selected Protection Clusters with Headquarters buy-in (agreement) from participating agencies.

Data management systems exist to support, not drive, how the humanitarian community assists survivors of human rights violations, and how survivors and their stories are protected. Moreover, the quality with which data management systems are designed and used in the field can impact survivors' experiences in reporting their incidents and with receiving services. It can equally impact the humanitarian community's understanding of the protection landscape in question. Therefore, it is imperative that the inter-agency community continues to reflect upon the challenges and recommended good practices for protection incident monitoring and case management systems, including those identified and outlined above.

While data sharing is important for protection strategies, community-level and global-level interventions, resource allocation, fund-raising and advocacy, the need for data must always be tempered with the rights of survivors to control how information about their respective protection incidents is used.