Guidance note on safe and ethical management, analysis and sharing of GBV service data in the context of integrated SRH-GBV programming

UNFPA

Funded by
the European Union

ACKNOWLEDGEMENTS:

The United Nations Population Fund (UNFPA) appreciates the support of the European Civil Protection and Humanitarian Aid Operations (ECHO) in funding this guidance note. The document was written by Christine Apio and Nadine Cornier from the Programme Support Unit (UNFPA). Thanks to the colleagues who guided and supported the process: Françoise Ghorayeb, Astrid Haaland, Rofand Khalaf, Kathleen Mitchell, Catrin Schulte-Hillen, Elisabeth Pender, Akiko Takano and the Regional Information Management Specialists from UNFPA.

DISCLAIMER:

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

© UNFPA 2026.

1. Introduction

Managing data related to gender-based violence (GBV), including data on survivors of sexual exploitation and abuse (SEA)[1], as well as data generated through the provision of sexual and reproductive health (SRH) services, is a sensitive and complex task.

In many contexts, limited service availability, impunity for perpetrators, weak legal frameworks for protection, the existence of mandatory GBV reporting laws in several countries, and the stigma and shame survivors may experience, contribute to low reporting rates. These realities make accurate and ethical data collection both challenging and essential.

Survivor-centred service delivery must always remain at the core of SRH and GBV programming. At the same time, collecting, documenting, processing, storing, analysing, and sharing service data safely and ethically is critical. When managed appropriately, data enhances the quality of care, improves coordination across health and protection systems, supports advocacy efforts, and informs evidence-based programming – all while minimizing risks to survivors and service providers.

In integrated SRH-GBV programming, where health and protection actors may both collect and access survivor data, harmonized standards and coordinated practices are critical. They ensure consistency, protect confidentiality, and safeguard the dignity and rights of survivors.

The GBV Minimum Standards[2] (Standard 14) stresses the importance of safe and ethical practices in collection and use of survivor data as a key component of GBV response. Inadequate or unethical data management can increase the risk of harm, breach survivors' trust, and undermine the credibility of service providers. Conversely, good data practices help uphold survivors' rights, improve services and ensure actors are accountable.

Purpose: This document aims to support organizations implementing integrated SRH-GBV programmes in humanitarian and development contexts to strengthen the safe and ethical management of GBV service data. It is not a guide for case management (also referred to as CM) processes, but rather a practical resource to translate GBV guiding principles and relevant fundamental data protection principles into operational practice while respecting diverse legal frameworks and organizational mandates, as well as raise awareness of common risks and harms, and provide tools and information to improve data handling. Ultimately, the guidance seeks to ensure that the collection and use of GBV service data enhances service quality, coordination and advocacy, while always safeguarding the rights, dignity and safety of survivors.

Although technical in nature, the document aims to be practical and accessible, serving both operational staff and decision makers, who are responsible for upholding safe and ethical data practices. While the focus is on humanitarian contexts, the principles and approaches are applicable to any context and are relevant for all survivors, regardless of their age, sex or gender identity.

Scope: This guidance focuses exclusively on individual-level data generated through integrated SRH-GBV services, such as case management, clinical management of rape (CMR), mental health and psychosocial support (MHPSS), and other protection services. It does not provide instructions on how to conduct case management itself, nor does it cover population-based data (e.g., prevalence studies), or research protocols. Instead, it highlights linkages with SRH services in integrated programming contexts, where SRH and GBV actors must apply the same high standards of data protection, confidentiality and survivor-centred principles. In practice, this includes joint service models such as one-stop centres or coordinated referral systems between SRH and GBV service providers, which require harmonized and consistent data protocols.

1 PSEA tip sheet

2 Gender-Based Violence AoR and Global Protection Cluster, *The Inter-Agency Minimum Standards for Gender-Based Violence in Emergencies Programming* (Geneva, 2019).

Note: The same ethical principles and guidance articulated in this document apply to the management of data involving male as well as child and adolescent survivors in the context of integrated SRH-GBV service delivery.

Intended audience: This guidance is designed for SRH and GBV service providers and programme managers, protection and case management staff, data focal points, and coordination actors engaged in integrated SRH-GBV programming in humanitarian settings. It is also relevant for policymakers, donors, and monitoring and evaluation specialists who oversee or support data systems.

This document was developed as an inter-agency reference. While different agencies and NGOs have data related guidance, there is no standard inter-agency guidance covering all relevant issues. Different issues are covered in different documents, including:

The Minimum Standards for GBV Programming in Emergencies

The Clinical Management of Rape and Intimate Partner Violence Survivors

PSEA policy

Personal data policy

2. Key concepts and definitions

Understanding foundational concepts is critical to implementing ethical data management practices. These definitions are central to safe and effective service data use:

- **Health records** document clinical care (e.g. medical history, treatment, forensic evidence), and health providers manage them under medical ethics and health information systems.
- **GBV case management data** records survivors' needs, risks and services provided, managed by caseworkers under GBV guiding principles and survivor-centred case management tools (such as the Gender-based Violence Information Management System [GBVIMS]/GBVIMS+). GBV case management data ensures safe, survivor-centred psychosocial and protection support.
- **GBV survivor data:** Information that is generated during the delivery of GBV-focused case management services. It may include survivor demographics, incident characteristics, the type of services provided, case status and referral outcomes. This data is typically collected by caseworkers, counsellors or protection actors during intake, follow-up or case closure. Survivor data may remain sensitive even if names or direct identifiers are removed, particularly in small or closed communities.
- **Personal data:** Any information relating to an identified or identifiable individual.
- **Informed consent:** A voluntary process where the survivor freely and voluntarily agrees to share information or participate in services based on a clear understanding of the purpose, benefits, risks and limitations. Consent must be specific (not general), time-bound, and revocable/withdrawn at any point. All relevant health and protection service options should be presented to the survivor. Consent should be documented using tools that are adapted to the context (e.g. written consent forms, oral consent scripts, visual aids).[3]
- **Informed assent:** The expressed willingness to participate in services. For younger children, who are by definition too young to give informed consent but are old enough to understand and agree to participate in services, the child's "informed assent" is sought.[4]
- **Information-sharing protocol (ISP):** A formal agreement between service providers that sets how, when and under what circumstances information about GBV survivors may be shared. An ISP establishes the rules, procedures, and safeguards for information sharing, including the purpose and types of information that may be shared, consent requirements, who may access or receive information, and the responsibilities of each party, with the aim of protecting the safety, confidentiality and rights of survivors and all those involved.
- **Integrated services:** Service delivery models where SRH and GBV services are provided in a coordinated manner, either in the same facility or through robust referral systems. Such integration requires shared protocols and joint safeguarding of survivor data. In integrated models (e.g. one-stop centres), both types of data may coexist, but they must be stored separately, adhering to strict confidentiality protocols.
- **Cross-sectoral data flows:** The movement of survivor information between actors in different sectors, such as health, protection and legal. These flows require clear consent processes, data minimization and joint accountability to protect confidentiality.

3 Detailed information about informed consent can be obtained from Gender-Based Violence AoR and Global Protection Cluster, *The Inter-Agency Minimum Standards for Gender-Based Violence in Emergencies Programming* (Geneva, 2019), p. 8.

4 Ibid.

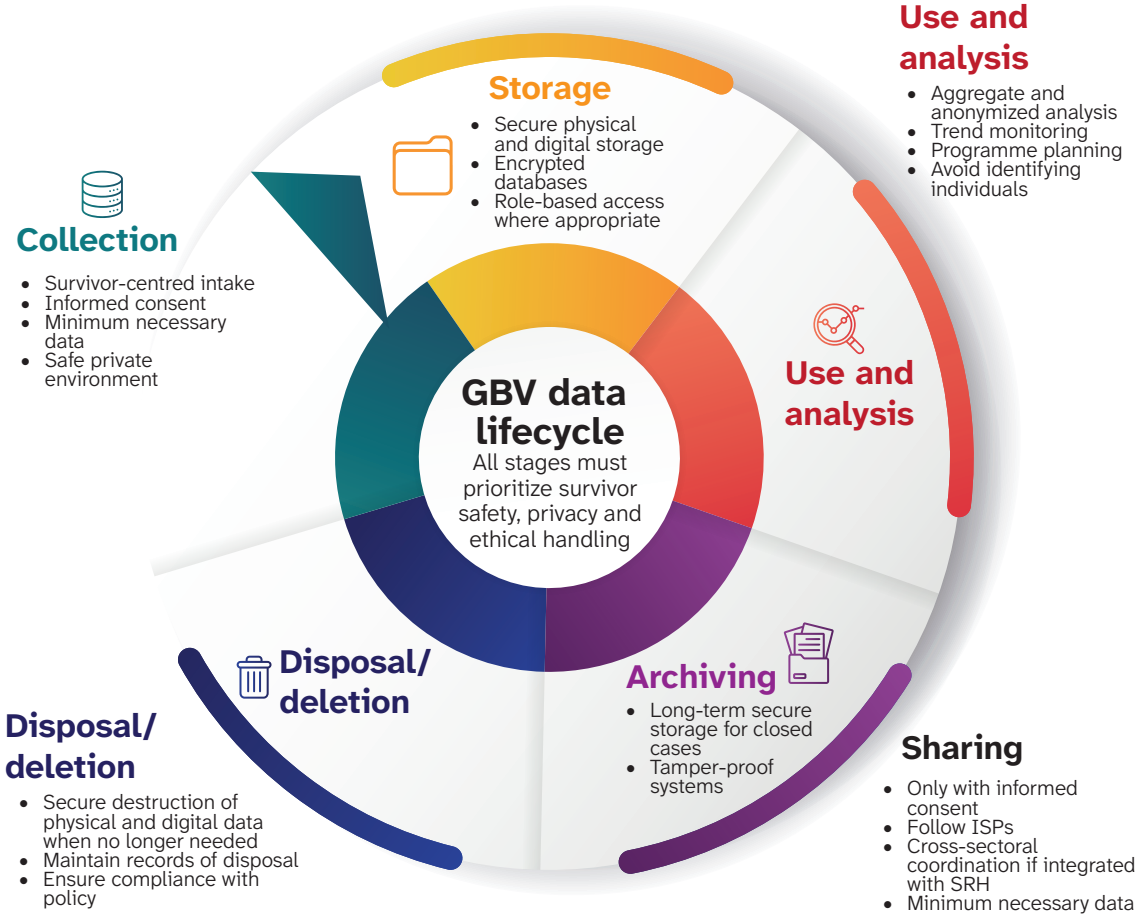
3. Guiding principles

Implementing safe GBV data practices requires adherence to internationally accepted principles. These should be embedded into all organizational policies, staff training and inter-agency coordination.

- **Survivor-centred approach:** All data practices must prioritize the rights, needs and choices of the survivor. This includes respecting their decisions about whether and how data is collected, stored or shared. Staff should communicate in a way that supports agency and dignity, especially with marginalized groups such as adolescents, people with disabilities, or survivors with diverse sexual orientations, gender identities, gender expression and sex characteristics (SOGIESC).
- **Confidentiality and informed consent:** The responsibility to protect a survivor's information from unauthorized access or disclosure. Confidentiality is a cornerstone of survivor trust and must be upheld in both formal documentation and informal communication. Breaching confidentiality, intentionally or unintentionally, can cause harm and legal repercussions. Staff must use consent tools that are adapted to the survivor's age, language, literacy level and cultural context. Informed consent should not be treated as a one-time form but as an ongoing conversation, with survivors encouraged to ask questions or change their minds.
- **Data confidentiality** must be maintained at all stages, from intake to storage to analysis. This includes avoiding unnecessary sharing, anonymizing data sets, and maintaining secure physical and digital storage systems. Confidentiality also applies during staff handovers or case transfers.
- **Do no harm:** Before collecting or using any data, staff should assess potential risks and put mitigation measures in place. This includes avoiding over-surveying survivors, preventing unauthorized access, and stopping data collection if it creates confusion or distress.
- **Data minimization:** The practice of collecting only the data that is strictly necessary for a defined, legitimate purpose (e.g. case management or service coordination). Data minimization reduces the risk of exposure and helps focus services on survivor needs rather than institutional requirements. Programmes should avoid collecting "nice-to-know" data and focus on "need-to-know" information. Reducing data volume not only protects survivors, but simplifies data management and lowers operational costs.
- **Accountability and transparency:** Organizations must have internal policies that define who is responsible for data management, how breaches are reported and how survivors can lodge complaints. Annual reviews or audits of data systems are recommended.
- **Integrated coordination and role clarity:** In contexts where SRH and GBV services are linked or co-delivered, ethical data management depends on clearly defining the roles of each sector. Programme managers or specialists should ensure that both SRH and GBV actors understand how survivor data is collected, shared and protected across service points. Joint training and harmonized procedures, such as shared consent forms or inter-agency ISPs, are essential to uphold consistent standards.

4. The data life cycle

Understanding the steps involved in data handling helps ensure consistency, security and compliance with ethical principles.



4.1 Collection: Managing and recording/documenting service data

- **Tools:** Use standardized intake, consent forms and case management tools (e.g. GBVIMS forms). These support consistency and quality and reduce the burden on staff and survivors. In integrated services, ensure SRH and GBV forms are aligned to avoid duplication and confusion.
- **Environment:** Conduct intake and data collection in secure, private settings to avoid breaches of confidentiality. Ensure both auditory and visual privacy so that survivors are not seen, overheard or interrupted while receiving services. This is also a standard of care in places where SRH services are provided.
- **Consent:** Explain why data is being collected, what it will be used for, who will have access and how it will be protected. Avoid medical or legal jargon. Seek informed consent for data collection. In joint SRH-GBV services, confirm that consent covers any cross-sector sharing or referrals.
- **Data quality:** Ensure accuracy and currency in documentation. Avoid assumptions or subjective language.
- **Data minimization:** Collect only the information needed to provide appropriate treatment and support. Avoid asking for sensitive information unless it is directly relevant to service provision. For example, it is rarely necessary to know the name of the perpetrator or exact location of the incident.
- **Non-verbal data:** Be mindful of non-verbal information (e.g. photos, audio), and avoid collecting such data unless absolutely necessary.

4.2 Data storage and access

- **Physical storage:** Store physical files in locked cabinets accessible only to authorized staff, in access-controlled rooms. Files should be labelled using codes, not names. In shared service settings, ensure that GBV case management files and CMR medical records are stored separately from other SRH files. Access to GBV case management and CMR medical records needs to be limited to authorised personnel.
- **Digital storage:** Use digital case management systems that are encrypted, password-protected and compliant with data security standards. Limit data downloads and require access permissions.
- **In all storage systems:** Store identifying information (e.g. name, contact info) separately from case details whenever possible.
- **Access control:** Limit access to sensitive data to those staff who need it to fulfil their job responsibilities. Implement role-based access levels. Ensure that only authorized and trained SRH staff can access GBV data. Regularly review and update access permissions. Ensure that sensitive clinical and GBV records are not removed from the service delivery site to avoid breaches in confidentiality.
- **Remote work considerations:** Ensure that laptops or mobile devices used in the field are secured and follow data backup protocols.

4.3 Data use and analysis

- **Anonymization:** Aggregate and anonymize data before using it for analysis, planning, visualizing or reporting.
- **Analysis:** Focus on trends that can inform programming (e.g. service utilization, time to referral) while avoiding patterns that could identify individuals. In integrated programmes, assess joint data to identify service gaps or referral delays across SRH and GBV entry points.
- **Limitations:** Be cautious when analysing service data for patterns or trends. Such data reflects only those who accessed services and does not represent GBV prevalence or incidence. Avoid misinterpreting trends.
- **Reporting:** Present findings in a way that protects survivors. For example, avoid disaggregating data to the point that individuals become identifiable. Use data to improve the quality and reach of services, strengthen case coordination, and inform strategic planning. Do not use service data to evaluate the performance of individual survivors or staff.

4.4 Data-sharing

- **With consent:** Obtain informed consent every time data is shared. When sharing for coordination or referrals, use only the minimum necessary data. This is especially important between SRH and GBV actors, who may have different mandates and confidentiality rules.
- **Via protocols:** Implement and adhere to information-sharing protocols that outline data-sharing safeguards including agreed formats, timelines and data limits. In integrated programmes, ISPs must be co-developed and signed by both SRH and GBV service providers.
- **Emergency sharing:** If required by law or in situations threatening the life or safety of the patient/survivor, data may be shared without consent. Only strictly necessary data may be shared. Whenever possible, a team decision should be sought. Due consideration should be given to the principle of acting in the best interests of the patient/survivor at all times.
- **Third-party requests:** Never share identifiable survivor data with external actors (donors, researchers, media, etc.) unless safety has been assured, and with explicit, documented consent.

4.5 Archiving and disposal

- **Retention policies:** Define a data retention policy based on legal, programmatic and safety considerations.
- **Archiving:** Use secure systems that preserve the integrity of archived data and prevent unauthorized alteration or deletion. Avoid storing inactive cases with active case files. Archive closed cases securely, ensuring they are protected from unauthorized access. In integrated service centres, clarify which agency is responsible for long-term archiving of survivor files.
- **Disposal:** Dispose of old files – physical or digital – using secure destruction methods when they are no longer needed. Use shredders, secure deletion tools or data-wiping software. Avoid informal disposal methods.

4.6 Mandatory reporting policies: Navigating mandatory reporting in SRH and GBV services

In certain contexts, there are mandatory reporting laws that obligate service providers to report to police or other government authorities. In such situations, survivors (and caregivers) should be made aware of these legal requirements as part of the informed consent process.[5] Mandatory reporting policies (laws requiring disclosure of GBV cases, especially sexual violence or cases involving minors) often put SRH and GBV actors in a difficult position, as they can both protect survivors and undermine survivor-centred principles (confidentiality, informed consent, autonomy). In contexts where such policies exist, SRH-GBV service providers must understand these legal frameworks to clarify what must be reported, by whom, and when. Mandatory reporting laws often create tension between legal compliance and survivor-centred care. Where SRH and GBV actors are required to comply with the law, they should take every step to minimize harm, uphold dignity, and protect survivor choice and safety. Strong internal protocols, survivor-informed communication and sustained advocacy are critical. When SRH-GBV service providers are unsure about what to do, they should seek further guidance and support from GBV and child protection specialized actors, as well as the protection cluster, for accurate interpretation and understanding.

There are specific mandatory reporting policies related to allegations of sexual exploitation and abuse involving humanitarian personnel. Mandatory reporting policies are intended to help escalate reports of SEA as quickly as possible to enable an organizational response. However, they can be difficult to reconcile with the survivor-centred approach and with the survivor's wishes and rights to autonomy. SRH and GBV actors should be familiar with the applicable reporting mechanisms and procedures, including who is responsible for receiving and acting on an allegation and what information may need to be shared. In these circumstances, survivors must be informed immediately upon reporting an incident when mandatory reporting procedures are in place. Do not 'promise' confidentiality as it is not acceptable to make promises to survivors that you might not be able to keep. Instead, from the outset, clearly explain what confidentiality means in the specific context, including its limits and any circumstances in which information may need to be shared without the survivor's consent.[6]

Protection from sexual exploitation and abuse (PSEA) networks and humanitarian country teams may require information to monitor trends, identify systemic risks and support sexual exploitation and abuse response, risk mitigation and prevention activities. For these purposes, data should be anonymized and only the required information should be shared. Where information is required for an investigation or accountability process, additional identifying information may need to be shared in accordance with the applicable procedures, legal requirements and data protection principles. Such information should only be accessed and shared by authorized persons for the specific purpose for which it is required.[7]

5 For more detailed information, see International Medical Corps, International Rescue Committee, UNICEF, UNFPA and UNHCR, *Inter-agency Gender-based Violence Case Management Guidelines: Providing Care and Case Management Services to Gender-based Violence Survivors in Humanitarian Settings* (2017), pp. 51–52.

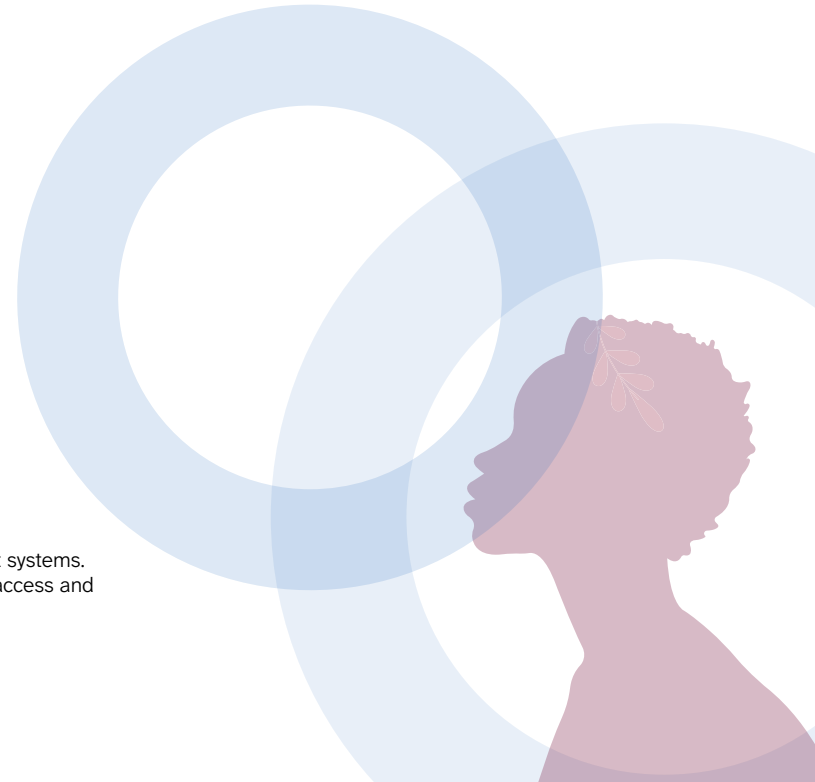
6 Mandatory reporting requirements can be in conflict with applying a survivor-centred approach, which seeks to empower the survivor by prioritizing her or his rights, needs and wishes, including the decision of whether or not to report sexual abuse.

7 Adapted from International Medical Corps, International Rescue Committee, UNICEF, UNFPA and UNHCR, *Inter-agency Gender-based Violence Case Management Guidelines: Providing Care and Case Management Services to Gender-based Violence Survivors in Humanitarian Settings* 2017, p. 51-52.

Spotlight on the GBVIMS and Primero/GBVIMS+

The 'legacy' GBVIMS, together with the digital platform Primero/GBVIMS+, are the only inter-agency endorsed tools for GBV information management in humanitarian contexts. They set the benchmark for safe, ethical and survivor-centred management of GBV service data. While designed for humanitarian settings, Primero/GBVIMS+ specifically is now increasingly being adapted for use within government and national structures to support sustainability. The legacy GBVIMS provides standardized incident monitoring, while Primero/GBVIMS+ builds on this to offer functions for case management documentation, outcome monitoring, performance indicator tracking, supervisory tools and a wider range of features to strengthen service quality. Both systems also support secure data storage and provide clear processes for the safe analysis and sharing of anonymized, aggregate data through agreed information-sharing protocols. Although GBVIMS and Primero/GBVIMS+ record only cases disclosed to trained service providers in the course of service delivery and should not be taken as prevalence or incidence data, they can generate valuable insights for integrated SRH-GBV programming, such as referral patterns and the timeliness of access to critical health services.[8]

To find out more about GBVIMS and Primero/GBVIMS+, visit www.gbvims.com.



8 Some GBV service providers may use other information management systems. These must follow the same principles of confidentiality, role-based access and survivor-centred data protection that underpin the GBVIMS.

5. Integrated services and cross-sectoral risks

5.1 SRH-GBV integration

- **Coordination:** In situations where services are integrated or closely linked, SRH and GBV actors should work together to identify relevant data points, each team collecting information that can inform complementary GBV and SRH programming, e.g. data points related to CMR service delivery. Ensure that data responsibilities are formalized in inter-agency standard operating procedures (SOPs) or referral protocols, and that role clarity is upheld at every stage of service delivery.
- **Cross-training:** Ensure that both GBV and SRH staff are trained in safe data practices and understand the limits of their roles. Provide joint training, when possible, to ensure mutual understanding of data protection roles. Consider including joint simulations or role-plays focused on referrals, consent and confidentiality to reinforce practice across teams.
- **Shared tools:** Ensure that referral forms and case notes are aligned and do not duplicate sensitive data unnecessarily. Avoid duplicating data collection across services. Ensure data entry is coordinated, and survivor consent is valid across sectors. Use harmonized consent language that explicitly mentions both SRH and GBV actors where relevant.
- **Survivor experience:** Where SRH services refer survivors to GBV case management (and vice versa), ensure that referral processes include clear consent steps, uphold confidentiality and do not contribute to trauma. Survivors should not have to retell their story multiple times unless they choose to. Data-sharing should aim to reduce burden, not add to it. Health and protection actors should coordinate closely to ensure that survivor dignity, choice and psychological safety are prioritized throughout the service journey.

Examples: Risks for GBV survivors in SRH services and mitigation tips

Risks:

- **Disclosure without confidentiality:** Survivors may share experiences during routine visits (e.g. antenatal care) in settings where privacy is lacking, risking stigma or unintended disclosure.
- **Mandatory reporting obligations:** Legal requirements to report without consent can deter survivors from seeking care or expose them to harm.
- **Limited GBV training for SRH staff and vice versa:** Staff may mishandle sensitive information or breach confidentiality, undermining trust.

Mitigation tips:

- Ensure private, safe spaces for survivor disclosure in SRH facilities.
- Clearly explain confidentiality limits and reporting obligations to survivors. Help protect the safety of the survivor by ensuring that survivors and GBV and SRH service providers are aware of the options to report sexual exploitation and abuse anonymously.
- Provide SRH staff with GBV-specific training on confidentiality, informed consent and survivor-centred care.
- Coordinate with GBV services for safe referrals while maintaining separate, secure records.

5.2 Referral systems and sharing

- **Informed pathways:** SRH and GBV actors should develop and implement ISPs at the inter-agency level to clarify referral pathways, data-sharing rules and survivor rights. Explain to survivors how referrals work, what data will be shared and what support to expect. Protocols should address specific integration points, such as SRH clinics referring survivors to psychosocial support or legal aid.
- **Timely consent:** Train staff to explain the referral process to survivors and obtain specific consent for each referral. Seek consent at the time of referral and document it. Use tools adapted for children or persons with disabilities as needed. Never share data with law enforcement or protection actors without survivors' consent, unless there is an emergency (life-threatening situation for a patient/survivor) or a specific legal or policy requirement (such as those related to SEA). Due consideration should be given to the principle of acting in the best interests of the client at all times. In one-stop centres or mobile clinics, ensure there are private spaces for confidential consent conversations even when multiple services are offered in the same location.
- **Feedback loops:** Where appropriate, establish feedback mechanisms between referral agencies to close the loop while maintaining confidentiality. These loops can be integrated into joint case conferences or cross-sectoral supervision meetings with strict confidentiality rules.

5.3 Legal and policy contexts

- **Compliance:** Organizations must comply with the applicable data protection principles, laws, and regulations when processing personal data (e.g., the UN Personal Data Protection and Privacy Principles, the UNFPA Policy and Procedures on Personal Data Protection, the EU General Data Protection Regulation [GDPR], the US Health Insurance Portability and Accountability Act [HIPAA], other relevant data protection and privacy laws). Understand applicable legal frameworks and policies on data protection, and mandatory reporting. Develop internal policies that align with legal obligations while prioritizing survivor safety. Integrated programming teams should jointly review relevant laws and map out shared compliance responsibilities.
- **Mandatory reporting:** If certain policies or the law requires mandatory reporting of certain incidents, both SRH and GBV providers should ensure that survivors are informed of this limit to confidentiality **before** services begin, as they might decide to decline the services to avoid reporting. Clarify in referral forms and consent scripts how mandatory reporting is handled across sectors (e.g. in health versus protection).
- **Legal aid:** Where survivors need legal assistance, integrate data-sharing into informed consent procedures. If referrals to legal services are made from SRH clinics, ensure health staff understand the appropriate limits and conditions for data-sharing.

6. Operationalizing safe data practices

Moving from policy to practice requires systematic support, training and accountability mechanisms:

Staff capacities

- All staff must be trained not only on technical tools, but also on ethical reasoning, cultural competence and survivor rights.
- Refresher training should be scheduled regularly, particularly when onboarding new team members or launching new tools.

Organizational policies

- Develop and enforce internal SOPs for data collection, storage and sharing.
- Conduct internal audits or peer reviews of data management practices.
- Assign data focal points or confidentiality officers in each team.

Monitoring and feedback

- Establish systems for survivors to provide feedback on how their data is handled.
- Include data protection indicators in regular monitoring and donor reporting.

Crisis scenarios

- Define emergency protocols (e.g. in case of data breach, device theft or internet shutdown).
- Ensure policies are in place for the safe and ethical closure of projects, including appropriate management and/or disposal of data and files.
- Ensure backup systems are in place and regularly tested.

Dos and don'ts

Do:

- Train all clinical and data staff on ethical data practices, including confidentiality, information security and survivor-centred communication.
- Ensure patient consent for relevant data collection (routine clinical data collection requires no consent).
- Use consent forms and scripts that are contextually appropriate.
- Ensure that all data-sharing or referral processes are consent-based and limited to the purpose of the referral.
- Ensure secure data storage physically and digitally, including for relevant health records.
- Limit data access to essential personnel.
- Limit access to sensitive data through role-based permissions.
- Develop and regularly review facility SOPs that define access, storage, sharing and retention procedures.
- Regularly review who has access to survivor data.
- Use anonymized aggregated data for reports and coordination.
- Conduct data practices audits to identify risks.

Don't:

- Assume survivors understand the risks without explaining them.
- Collect unnecessary or overly detailed personal data.
- Use survivor stories without a prior risk assessment, informed consent and anonymization (unless the survivor explicitly requests to be identified).
- Share identifiable information over email or messaging apps, or in casual conversation.
- Store sensitive data in unsecured systems.
- Use data to measure staff performance.
- Assume service data reflects GBV prevalence.

Example dilemmas and how to respond

Implementing ethical data practices can be complex in real-world situations. Below are common dilemmas and practical ways to respond while adhering to core principles of survivor safety, confidentiality and informed consent.

Dilemma 1: Incomplete consent for case notes

A caseworker did not ask a survivor whether her case information could be shared with a health referral partner. Now the referral is urgent.

Response: If possible, re-contact the survivor to seek informed, specific consent for the referral. If consent cannot be obtained and there is imminent risk to health or life, share only the minimum necessary data to ensure care, while documenting the rationale. Afterwards, conduct a supervision review to prevent recurrence.

Dilemma 2: Healthcare provider requests case notes from GBV case manager

A health clinic treating a survivor of sexual violence requests her full GBV case file from the GBV case manager to "better understand the situation."

Response: Full case notes should not be shared, even with other trusted service providers, unless the survivor has provided specific, informed consent for that purpose. Instead, share only the information directly linked to improving the survivor's care. Ensure that staff from both sectors are trained on data protection protocols, and that standardized referral forms guide what information is shared. Confirm that both parties follow a shared ISP.

Dilemma 3: GBV case manager requests medical records from healthcare provider

A GBV case manager wants to follow up on a survivor's referral to a health clinic and asks the provider to share the medical report to complete her case file.

Response: Health data is highly sensitive and protected by medical confidentiality. Medical staff cannot share clinical records with non-health actors unless the survivor has given informed, explicit consent. To handle this ethically, the case manager should first ask the survivor whether she agrees to share medical information, and for what purpose. If the survivor consents, this should be documented and include what data will be shared and with whom. The health provider should then share only the relevant information, ideally using a summary or referral form, not the full medical record. This type of sharing should be covered under the ISP and supported by joint SOPs or referral protocols.

Dilemma 4: Mandatory reporting policy

A 16-year-old girl seeks medical services from a health facility following an incident of rape. She does not want the incident reported to the police out of fear of retaliation and stigma. However, national law requires mandatory reporting of all cases of sexual violence involving minors to law enforcement. The health service provider faces a conflict between upholding the survivor's confidentiality and autonomy and compliance with mandatory reporting laws.

Response: Explain mandatory reporting requirements as they apply in your local setting, clearly communicating what must be reported by law and why. When possible, explain these requirements before the patient/survivor discloses information that might require reporting. Due consideration should be given to the principle of acting in the best interests of the patient/survivor at all times. Engage a GBV or child protection focal point or protection actor for case-by-case guidance on legal obligations and survivor safety.

7. Resources and tools

- GBVIMS tools – Intake forms, consent forms, user guide
- Gender-Based Violence AoR and Global Protection Cluster, *The Inter-Agency Minimum Standards for Gender-Based Violence in Emergencies Programming* (Geneva, 2019) – Standard 14 on collection and use of survivor data
- WHO, *WHO Ethical and Safety Recommendations for Researching, Documenting and Monitoring Sexual Violence in Emergencies* (Geneva, 2007) – Guidance on researching, documenting and monitoring sexual violence in emergencies
- International Medical Corps, International Rescue Committee, UNICEF, UNFPA and UNHCR, *Inter-agency Gender-based Violence Case Management Guidelines: Providing Care and Case Management Services to Gender-based Violence Survivors in Humanitarian Settings* (2017), pp. 51–52
- Gender-Based Violence AoR and Global Protection Cluster, *Handbook for Coordinating Gender-Based Violence Interventions in Emergencies* (Geneva, 2019), p. 39
- UNFPA/GBV AoR Resource Pack – Videos, podcasts and case studies
- GBV information-sharing protocol templates – Inter-agency sample documents
- UNFPA, *Guidance on the Safe and Ethical Use of Technology to Address Gender-based Violence and Harmful Practices* (New York, 2023)

For more support, contact global/regional UNFPA SRHiE/GBViE focal points.

Guidance note on safe and ethical management, analysis and sharing of GBV service data in the context of integrated SRH-GBV programming

Produced by:
United Nations Population Fund
Humanitarian Response Division
Geneva, Switzerland

Funded by
the European Union