



# THE ANNOTATED PROTOCOLS GUIDE

Project Roadmap created annotated protocols in response to regular requests for resources and support. ECM Coordinators/Directors, who often take a leadership role in creating written protocols, along with other subject matter experts, also helped to inform this guide.

This series of annotated protocols offers practical guidance, sparks meaningful discussion, and serves as a reference for both the content and scope of effective protocols. Each numbered heading outlines key elements to consider, explains their significance, and provides sample language to help task forces tailor protocols to their unique needs.

## Why Protocols Matter

In the early stages of a multidisciplinary task force's development, it is common for members to question the need for formal or extensive protocols especially as they are still evolving. Although protocol development may seem unnecessary at first, it is critical for consistency, longevity, and sustainability.

### Protocols help task forces:

- Build transparency and trust among members
- Avoid tension and misunderstandings
- Provide a clear process for addressing any conflict
- Establish clear accountability
- Ensure fair and consistent decision-making

Whether your ECM task force is just beginning or refining long-standing practices, this guide can help facilitate thoughtful conversations and intentional planning around protocol development.

## Annotated Protocols

- Information Sharing
- Membership
- **Data Collection**
- Decision Making



### Additional Protocol Development Resources

[\*Enhanced Collaborative Model \(ECM\) Anti-Human Trafficking Task Force Protocol Development Checklists\*](#)

[\*Human Trafficking Task Force Protocol Development Training Video Series\*](#)

[\*Multidisciplinary Collaborative Model for Anti-Human Trafficking Task Forces: Development and Operations Roadmap\*](#)

---

## Task Force Data Collection Protocol (Annotated Example)

Below is an annotated example protocol for data collection within a multidisciplinary human trafficking task force. Each provision begins with an explanation as to why that information is relevant/important and is followed by sample language. This is a tool, that when combined with other resources and discussion, will help task forces develop protocols that suit the needs of their circumstances.



### 1. Purpose and Scope

Starts with a clear purpose to remind members why data collection matters. Links it to the mission, grant accountability, and internal learning – not just compliance.



**Sample Language:** This protocol outlines the task force’s process for collecting and managing data related to human trafficking investigations, victim services, outreach, and training. It supports compliance with federal grant reporting requirements (e.g., the Office for Victims of Crime Performance Management Tool (OVC PMT)) and informs internal planning, performance monitoring, and systems improvement.

---

**Note:** The purpose and scope of data collection can vary greatly depending on your jurisdiction and resources.

---



### 2. Protocol Created By

Names who designed the protocol to signal legitimacy and build buy-in. Shows cross-disciplinary input, which encourages adoption and helps prevent bias toward one sector’s norms (e.g., law enforcement vs. victim services).



**Sample Language:** This protocol was developed collaboratively by the task force, with input from task force members.



### 3. Who Collects Data and Why

Clearly defines who is responsible for data collection to ensure shared responsibility across disciplines – not just the Coordinator/Director. This builds ownership and consistency.



**Sample Language:** Data is collected by individuals and entities engaged in task force related activities. Each collector is responsible for recording universal data categories and/or data relevant to their role in alignment with this protocol.

---

**Note:** Consider using your Memorandum of Understanding (MOU) to define what data each member should collect. Some task forces have “universal data” that all parties to the MOU agree to collect (ex: training data), and some do not.

---



## 4. What Data Is Collected

Clarifies what data you need to collect and why. Avoids collecting “everything just in case.” This keeps partners from feeling overwhelmed and improves data/reporting quality.



**Sample Language:** The task force collects data aligned with its mission and goals, as well as program goals and federal reporting guidelines where applicable.

---

### Informed Consent

Remember to include informed consent in your data protocol and process for times when the task force (not the VSP in its own course of business) wants to collect or use victim data. The protocol should clearly specify when victim consent is required and how consent will be obtained and documented.



## 5. How Data is Collected

Clearly outlines how and where the task force will collect data. Avoids assumptions that people know how or where to report. This section addresses practical logistics and builds standardization across agencies.



**Sample Language:** Partners will use standardized templates and forms to ensure consistency and accuracy of data. Definitions, forms, and links will be provided to those who are collecting data on behalf of the task force.

**Note:** To clearly outline how/where data will be collected, the task force should work together to develop templates or forms for data reporting/collection. In addition, how data is collected is different than how organizations then share that data with the aggregate.



## 6. Data Governance: Storage, Confidentiality and Access

Language in this provision reassures partners that you are protecting survivor data. Connect this to a broader confidentiality protocol for credibility and compliance.



**Sample Language:** All sensitive data will be stored securely on encrypted platforms with role-based access. Personally identifiable information will not be shared in aggregate reporting. A companion confidentiality protocol governs de-identification and ethical use of data.



## 7. Shared Definitions and Data Dictionary

Uses shared definitions to prevent misreporting. A data dictionary is especially helpful when partners use different systems or languages.



**Sample Language:** The task force uses a shared data dictionary, developed collaboratively, and includes definitions for OVC PMT reporting. The data dictionary is connected to the form(s) used for data collection to reduce margin for error.



## 8. Deadlines and Reporting Cycle

Builds in clear reporting cycles and expectations. This helps with accountability and makes data review a regular habit – not a last-minute scramble.



**Sample Language:** Partner agencies are expected to report data monthly or communicate to the main point of contact when there is no data to submit. While the task force has ECM funding, the task force reports grant data to the OVC PMT quarterly.



## 9. Data Use, Review and Dissemination

Specifies how data will be reviewed, disseminated and used. Clearly communicates to partners the intended purposes of data collection – beyond compliance – and identifies both allowable and prohibited uses to support transparency, trust, and responsible data stewardship.

**Example:** Collected data supports the following activities:

- Strategic planning and needs assessments
- Identifying service gaps and strengthening coordination
- Public-facing storytelling, media engagement, and funding or advocacy efforts, where appropriate, and subject to task force defined parameters to prevent misuse and protect victims and partners
- Grant reporting and compliance



## 10. Partner Agreements

Including data collection in MOUs elevates its importance and formalizes expectations of participation, provides for consistency, and builds confidence in the security of data collection.



**Sample Language:** Expectations for data collection, reporting, and use are incorporated into the task force's MOU.



## 13. Ownership, Review, and Revision

Builds sustainability and responsiveness.



**Sample Language:** The protocol will be reviewed annually and agreed-upon updates will be made by the Coordinator/Director. Updates will be made in response to new laws, challenges, or partner input.

---

### APPENDIX A: Tiered List: Types of Data a Task Force Might Collect

This list is structured in three tiers – ranging from basic operational data to sensitive victim-level details requiring consent.

When considering and defining the data the task force will collect, there are several helpful considerations:

1. What data do funders require for performance measurement or for completion of deliverables? For example: OVC collects specifically outlined data in PMT.
2. Are there other data the task force would benefit from collecting, even if not required by funders?
3. Are there any laws or ethical considerations the task force should be aware of that might constrain or guide what data is collected?

#### Tier 1: Basic and Operational Data (No Identifying Information)

Collectable by most partners without confidentiality concerns.

- Number of referrals made/received between partners
- Types of services provided (e.g. age range, sex, nationality)
- Case status (open, closed, referred)
- Number and types of outreach events conducted
- Number of training sessions delivered by audience
- Number of potential or confirmed trafficking cases opened during reporting period
- General location of case activity (e.g. county or zip code)

## Tier 2: De-Identified or Shared with Limited Access

Requires agreed definitions, possible agency MOUs, and protocols to protect confidentiality.

- Survivor experience categories (e.g. sex trafficking, labor trafficking, or both)
- Services requested or declined
- System involvement (e.g., child welfare, criminal justice)
- Known risk factors (e.g., homelessness, immigration status, gang involvement)
- General timeline of victim engagement (e.g., how long to access shelter)
- Basic indicators from victim screening tools, anonymized

Best practice: Report in aggregate or anonymized form. Access should be limited to relevant personnel.

## Tier 3: Personally Identifiable or Highly Sensitive Information

Requires explicit, informed victim consent, and strong legal and ethical protections.

- Survivor name, birthdate, or social security number
- Case narratives, direct quotes, or detailed trafficking experiences
- Medical records or diagnoses
- Immigration or legal status
- Criminal history (victim or trafficker)
- Exact addresses, phone numbers, or employer details
- Law enforcement interview transcripts or recordings
- Active safety concerns or protection orders
- Mental health or substance use treatment records

Note: Unless required for case coordination or service delivery – and with consent – this type of data should not be shared across agencies.

## Final Considerations for Task Forces

- Start with Tier 1 data to build comfort and consistency in sharing.
- Use MOUs to clarify expectations and protect sensitive info.
- Always prioritize informed consent and survivor autonomy—even if the law allows sharing.
- Consider creating a “Data Menu” that partners can select from when reporting or engaging in collaboration.