ARCvi | Actionable Resources for Change in Violence Intervention

Temple University College of Liberal Arts | Public Policy Lab

July 2026

Quick Guide: Drafting Data Sharing Agreements for Service Providers

Guidance for CVI programs sharing participant information with referral agencies and service partners

✓ **Purpose:** This guide addresses service coordination—not research consent. It helps CVI providers structure written agreements and participant authorization forms while protecting autonomy, safety, and privacy.

Why written agreements matter

CVI programs often coordinate with hospitals, behavioral health providers, housing and workforce programs, victim-service organizations, schools, and other partners. Information sharing can improve referrals and continuity of care, but it can also create risk when participants do not understand what will be shared or agencies have different expectations about access, security, and follow-up.

A written agreement defines the purpose and limits of sharing before information moves between organizations. It should protect participant choice and clarify how each agency will access, use, store, correct, retain, and disclose information.

↔ **Two documents may be needed:** A provider-to-provider agreement sets the rules agencies will follow. A participant authorization or release-of-information form (signed by the participant) records permission for specific information to be shared. One does not automatically replace the other.

Start with six principles

- Share for a defined participant-service purpose—not because information might be useful later.
- Use the minimum information needed for the referral, coordination, or safety purpose.
- Use informed and voluntary authorization whenever the law permits participant choice.
- State clearly what may be shared, what may not be shared, and whether it may be shared again.
- Consider whether disclosure could create retaliation, stigma, legal exposure, family conflict, or other harm.
- Review agreements when partners, technologies, services, funder rules, or laws change.

Before drafting, ask:

? Why is the information needed, and how will sharing benefit the participant?
? Is identifiable information necessary, or could less detailed information meet the need?
? Which organizations and staff members truly need access?
? What laws, contracts, funder conditions, and professional standards apply?
? What will happen if the participant declines or later revokes authorization?

What to include in a provider-to-provider agreement

The agreement between organizations should describe the relationship, permitted data uses, and safeguards each party will maintain. The detail should match the sensitivity and frequency of sharing.

1 Parties and purpose

Name each organization and the referral, coordination, safety-planning, or other authorized purpose.

2 Data covered

List the fields or record types that may be exchanged and information that is excluded.

3 Roles and access

Identify who may send, receive, view, enter, correct, download, or print information.

4 Participant authorization

State when authorization is required, who obtains it, where it is stored, and how revocation is communicated.

5 Security safeguards

Define approved transmission and storage methods, access controls, staff training, and protections for paper records.

6 Use and redisclosure limits

Restrict use to the agreed purpose and prohibit further sharing except as authorized or legally permitted.

7 Accuracy and correction

Explain how errors will be corrected and when partners must be notified of changes.

8 Retention and destruction

Set retention periods and secure destruction procedures for electronic and paper copies.

9 Breach response

Set timelines and contacts for unauthorized access, disclosure, loss, or other privacy incidents.

10 Review and termination

Explain how the agreement is amended, reviewed, ended, and how data are handled afterward.

Core fields in a participant authorization form

Use plain language and enough detail for the participant to understand exactly what is being authorized. Depending on the services and information involved, include:

- ☐ Participant name and date of birth
- ☐ Name of the CVI organization releasing information
- ☐ Specific agency or agencies receiving information
- ☐ Whether sharing is one-way or permits mutual communication
- ☐ Specific information that may be shared
- ☐ Purpose of disclosure: E.g., referral, service coordination, or safety planning
- ☐ Information that may not be shared
- ☐ Effective date and expiration date or event
- ☐ Statement that authorization is voluntary
- ☐ How the participant may revoke authorization
- ☐ Whether refusal affects services
- ☐ Limits on redisclosure
- ☐ Participant or guardian signature, staff signature, date

i

Distinguish direction of sharing: A one-way authorization allows one organization to disclose information to another. Mutual communication allows identified organizations to exchange information in both directions. State this clearly.

Participant-centered practice

i

Explain before asking for a signature: Review the form with the participant, describe potential benefits and risks, answer questions, and provide language or accessibility support when needed. A signed form is not a substitute for understanding.

Build meaningful choice into the process

- Allow participants to authorize some categories of information while declining others when feasible.
- Avoid broad terms such as “all records” unless they are necessary and legally appropriate.
- Do not combine unrelated purposes into one blanket authorization.
- Give the participant a copy and identify whom to contact with questions.
- Create a reliable process for recording and communicating expiration or revocation.

Special categories require added review

A qualified privacy officer, attorney, or other knowledgeable reviewer should examine the final documents, particularly when information involves:

- Minors or guardianship questions
- Medical or behavioral-health records
- Substance-use treatment information
- Victim services, domestic violence, sexual assault, or stalking
- Justice-system or supervision records
- School or educational records
- Immigration, housing, or other information that could create legal or safety risk

! **Important:** Federal and state rules differ. HIPAA authorizations have required elements, and certain substance-use treatment records receive additional protection under 42 CFR Part 2. Victim-service and youth records may also have specialized confidentiality rules. A general release form may not be sufficient for every record or partner.

Final review checklist

☐ The purpose is specific and connected to participant services.
☐ Only necessary information is included.
☐ The participant can identify every organization allowed to exchange information.
☐ The form distinguishes one-way release from mutual communication.
☐ The effective period and expiration date or event are clear.
☐ The process for revocation is practical and documented.
☐ The provider agreement addresses access, security, redisclosure, accuracy, retention, and breach response.
☐ The participant receives an explanation and a copy of the signed form.
☐ The final documents have been reviewed for applicable legal, contractual, and funder requirements.

ARCvi takeaway

★ Good data sharing is not about exchanging as much information as possible. It is about sharing the right information, for a clear purpose, with participant understanding and strong safeguards.

Selected authoritative guidance: U.S. Department of Health and Human Services guidance on HIPAA authorizations and privacy; Substance Abuse and Mental Health Services Administration guidance on 42 CFR Part 2; and applicable federal, state, local, contractual, and professional requirements.

Disclaimer: This quick guide provides general educational information and is not legal advice. Organizations should tailor documents to their services, participants, partners, technologies, funding conditions, and jurisdiction.