

Cross-System Data Sharing & MOU Checklist

A Practical Planning Guide for HMIS and
Community Partners



A Practical Planning Guide for HMIS and Community Partners

Use this checklist to identify the decisions your partners should work through before information moves between systems or a Memorandum of Understanding is signed.

Created by Bitfocus for HMIS administrators, Continuum of Care leaders, legal and privacy teams, healthcare partners, social-service agencies and technology teams preparing for cross-system data sharing.

Before You Begin

Cross-system data sharing can improve coordination and reduce repeated data entry. Siloed systems shift system friction onto clients, leading to repeated intake, the retelling of traumatic history, and slower housing placement. By moving to shared stewardship, communities can treat data as a community asset held in trust, rather than a private possession.

Before systems connect, partners need agreement on purpose, consent, access, responsibility and risk. Most projects stall on uncertainty, not on the law itself. The goal here is to translate legal constraints into operational rules, roles, and workflows.

Use this checklist to identify what is settled, what still needs an owner and what requires legal or privacy guidance.

This resource supports planning conversations and is not legal advice.

Define the Purpose and Partners

What should this connection accomplish, and who needs to be involved?

A strong agreement begins with a shared purpose and clearly identified partners.

Questions to Discuss

- What problem are we trying to solve?
- Who should benefit from the shared information?
- Which organizations will provide, receive or act on the information?
- Who can approve the agreement for each organization?
- Who will make day-to-day operational decisions?
- How will the partners know whether the connection is working? (e.g., measuring time from referral to housing placement, duplicate intake reduction, or consent completion and renewal rates)

Decisions to Record

Primary purpose:

Participating organizations:

Named decision-makers:

Desired outcome and success metrics:

Define the Information and Its Use

What will be shared, and what may partners do with it?

Avoid broad descriptions such as “client data.” Be specific about the information, systems and intended uses.

Questions to Discuss

- Which data elements will be shared?
- Which system is the source of record?
- Which system will receive the information?
- Will information move in one direction or both?
- How often will it move?
- Which roles may access it?
- Which uses are permitted?
- Which uses are prohibited?
- How long may each organization retain it?

Decisions to Record

Information to be shared:

Source and receiving systems:

Approved uses:

Prohibited uses:

Plan for Consent, Privacy and Governance

How will clients be informed, and who controls access and use?

The agreement should reflect the legal and privacy requirements that apply to the participating organizations and information.

These may include HIPAA, 42 CFR Part 2, state or local requirements and organizational policies. Apply the strictest applicable rule to each data element. Do not assume health-privacy rules block all sharing, but treat protected substance-use-disorder data as the highest-constraint category when applicable.

Questions to Discuss

- When is client consent required?
- How will clients understand what is being shared and why?
- Will staff have standard scripts for explaining consent to ensure clients can make informed choices without confusion?
- Can consent be captured on a single screen to reduce staff burden and prevent workarounds?
- Where will consent be recorded?
- How will partners respond when consent is withdrawn?
- Who approves access?
- How often will access be reviewed?
- Who can approve a change in scope or permitted use?
- How will disagreements be resolved?

Decisions to Record

Applicable legal and privacy requirements:

Consent process:

Access approval process:

Governance lead or group:

Assign Responsibility and Manage Risk

Who is responsible when information is wrong, misused or exposed?

Partners should know who manages corrections, access concerns, incidents and shared risk before the exchange begins.

Questions to Discuss

- Who corrects inaccurate or duplicate information?
- Who investigates suspected misuse?
- How will privacy or security incidents be reported?
- Who leads the response to a breach or improper disclosure?
- Who communicates with affected clients?
- How will responsibility and risk be shared?
- How will security expectations match system administration to data sensitivity and partner roles?

Decisions to Record

Data-correction owner:

Incident-response lead:

Client-notification responsibility:

Questions requiring legal review:

Security expectations and role mapping:

Define the Technical and Operating Plan

How will the connection run, and what happens when it fails?

The agreement should establish how information will move, who will monitor the exchange and how changes or failures will be handled.

Questions to Discuss

- Which systems and technical tools will be used?
- Will the exchange be real-time, scheduled or manual?
- Who monitors failures, delays or incomplete records?
- Who provides technical support?
- How will changes be tested?
- How will partners prevent duplicate or conflicting records?
- What happens if one system becomes unavailable?
- Which staff members need training?

Decisions to Record

Technical approach:

Monitoring and support owner:

Failure and escalation process:

Training and documentation owner:

Plan for Review and Change

How will the agreement evolve as programs, partners and requirements change?

Data-sharing agreements should not remain static while the systems and organizations around them change.

Questions to Discuss

- How often will the agreement be reviewed?
- Who may request a change?
- How will amendments be approved?
- What happens when a partner joins or leaves?
- How will access be removed?
- How will the exchange be paused or ended?
- What happens to shared information after termination?

Decisions to Record

Review schedule:

Amendment process:

Partner exit process:

Retention or deletion requirements:

Final Readiness Check

Before the agreement moves forward, confirm that:

- The purpose and intended outcome are clear
- Every participating organization has a named decision-maker
- The information being shared is specifically defined
- Permitted and prohibited uses are documented
- Consent and privacy requirements have been reviewed
- Access and governance responsibilities are assigned
- Correction and incident-response processes are clear
- The technical approach and support responsibilities are defined
- Review, amendment and termination processes are documented
- Unresolved legal and privacy questions have been referred to qualified counsel

Next Steps

Review the checklist with representatives from:

- HMIS administration
- Program leadership
- Legal and privacy
- Technology and security
- Data and reporting
- Participating community partners

Mark what your group can answer now, assign an owner to unresolved decisions and identify the questions that require additional guidance.

About Bitfocus

Bitfocus is the technology partner behind Clarity Human Services, an HMIS platform built for communities coordinating housing, services, referrals and homelessness-response data.

Bitfocus works alongside HMIS administrators, Continuum of Care leaders and community partners to strengthen data governance, interoperability, reporting and everyday system operations.

[Schedule a Clarity Human Services Demo](#)