COMMUNITY VIOLENCE INTERVENTION (CVI) PRIVACY & TRUST FAQ

Best Practices Guide Prepared for End Community Violence Now (ECVN) and Coalition Partners

ECVN works in collaboration with survivors, community organizations, public health partners, law enforcement, and policymakers to advance evidence-based solutions to gun violence. This FAQ provides practical guidance to help coalition partners protect participant trust, maintain ethical boundaries, and safely collaborate across sectors (including government and law enforcement) while delivering services intended to reduce harm, prevent and intervene in violence, and support community well-being through strategies grounded in public health, community trust, and accountability.

1. Why is this guidance important?

Across the nonprofit sector, organizations are grappling with increasingly important privacy obligations and heightened expectations regarding how they handle personal information, including the need to do so in a transparent and accountable manner. CVI programs in particular depend on trust, psychological safety, and voluntary engagement. Participants often share sensitive personal information because they are seeking support, stability, or protection. If participants believe their information could be used for enforcement or surveillance purposes, they may disengage from the program altogether, even if no disclosure actually occurred, which weakens safety outcomes and violence prevention efforts. Therefore, preserving the confidentiality of sensitive information and maintaining participant trust is not only a legal obligation, it is also essential to program effectiveness.

2. Can CVI programs work with law enforcement?

Yes, effective CVI models include a healthy working relationship with law enforcement, but the roles must be clearly defined and transparent. Effective partnerships clearly define the role of each partner, communicate boundaries to program participants, explain when law enforcement is involved, and specify what information is shared (and what is not shared). When boundaries are unclear, trust erodes even if no rules were technically broken.

3. What is the biggest risk to avoid?

Blurred roles present the greatest risk to CVI programs in the current environment. Problems arise when service providers also act as investigators, when law enforcement volunteers have access to participant data, when affiliations are not disclosed, and when participants believe services are confidential but they are not. Undisclosed affiliations can create perceived coercion or surveillance risks and undermine program credibility. Programs should require disclosure of conflicts of interest and affiliations. Participants should not have to guess whether they are speaking to program partner personnel in their capacity as a service provider or as law enforcement. As noted above, even the perception of unclear boundaries can erode trust and reduce program effectiveness.

4. What information should be collected from participants?

Organizations should collect only the information they actually need. Best practices require collecting the minimum necessary data, avoiding sensitive details unless they are essential, and refraining from collecting information that the organization cannot safely protect.

5. What is considered "protected participant information" that should be treated as confidential?

Protected participant information includes any personal, program, safety-related, legal, or health information about a CVI participant that could identify them or expose them to risk if disclosed. At a minimum, CVI programs should treat the following as protected participant information:

a. **Personally Identifiable Information** (*e.g.*, participant name, address, phone number, date of birth, SSN, family relationships, and photographs or identifying images);

b. **Program Participation Information** (*e.g.*, intake forms, case management records, participant rosters, service plans, attendance at outreach or mediation sessions);

c. **Sensitive Safety-Related Information** (*e.g.*, conflict mediation details, threat or retaliation information, group affiliation discussions, safety plans, locations of meetings or outreach activities);
d. **Justice System Information** (*i.e.*, information relating to participants' interactions with the criminal justice system);
e. **Health and Trauma-Related Information** (*e.g.*, mental health information, trauma history, substance use treatment, and other medical information); and
f. **Immigration or legal status**.

Nonprofits should collect only the data they actually need and avoid unnecessary tracking or sharing.

6. When can protected participant information be shared with law enforcement?

Protected participant information should not be shared with law enforcement *unless*:

a. The participant has provided **clear** and **informed consent**;
b. A **specific legal requirement** applies (*e.g.,* mandatory reporting law or judicial warrant); or
c. There is an **immediate safety risk** that justifies an emergency exception.

Participants need to know in advance who will receive their information and why. Routine or informal sharing, sometimes described as "relationship-based sharing," should not occur. Organizations should document the legal basis for any disclosure.

7. What should CVI programs disclose to program participants at intake?

Participants should understand the identity and purpose of the organization conducting the CVI programming, as well as any relevant affiliations the organization has within the CVI ecosystem. Participants should also know what information the organization is requesting, why it is needed, and how it may be used, including for service delivery, reporting requirements, and situations where disclosure may be legally required. Privacy expectations should be explained clearly and repeatedly, not just once.

8. What does valid participant consent look like?

Valid participant consent must be:

a. **Voluntary**, meaning that services cannot depend on agreeing to share information;
b. **Informed** and **specific**, clearly identifying who will receive what information;
c. Presented in **plain language** and be **understandable**, rather than buried in lengthy legal forms;
d. **Revocable**; and
e. **Obtained before any disclosure occurs**.

In addition, participants must understand whether law enforcement partners exist, whether data will ever be shared, and what happens if they decline. Organizations should maintain procedures for collecting consent and honoring participant rights.

9. What are "firewalls" and why do they matter?

A firewall is a structural separation between service provision and enforcement functions. It ensures that service providers do not function as intelligence gatherers. In practice, this means that law enforcement partners do not have unrestricted access to participant records, disclosure is restricted unless legally required, written memoranda of understanding define roles and boundaries, law enforcement partners do not volunteer in roles involving confidential participant conversations, shared meetings exclude confidential participant details, and data systems include restricted access controls. Clear separation protects both participants and staff.

10. How should organizations store and protect data?

Organizations should implement secure storage systems, restrict access to information based on role, provide regular staff training, and maintain breach response plans. Strong security safeguards are expected of nonprofits that handle

personal data. Participant information should be retained only as long as necessary for program operations or legal requirements. Organizations should implement written records retention policies and delete unnecessary data.

11. Should staff disclose affiliations?

Yes. Anyone with law enforcement or investigative authority should disclose that affiliation when interacting with participants. Participants should never later discover that a trusted service provider also held an enforcement role. As stated above, undisclosed affiliations can undermine community trust even when no wrongdoing occurred.

12. How should organizations address immigration concerns?

Participants may fear that their data will be shared with ICE or other federal authorities. Programs should avoid collecting immigration status information unless it is necessary, clearly explain the limits of confidentiality, refrain from promising protections they cannot guarantee, and provide alternative participation options where possible. Trust depends on honest communication, not reassurance alone.

13. What policies should organizations consider having in place?

Organizations should review and consider the need for adopting an information security and data privacy policy, intake and informed consent procedures, conflict of interest disclosure procedures, records retention policy, and a written law enforcement partnership memorandum of understanding (as needed). Organizations should also map what data they collect and clearly document why they collect it.

14. What training should organizations provide to staff?

Staff and volunteers should receive ongoing training on confidentiality, informed consent, trauma-informed communication, and the handling of sensitive data. Regular training helps maintain compliance and protects participants.

15. How should intake be conducted?

Intake should be conducted using trauma-informed practices. Staff should explain confidentiality before asking sensitive questions, ask only necessary questions, allow participants to skip questions, avoid collecting information "just in case," and never imply that participation requires cooperation with law enforcement requests. Collecting unnecessary personal data increases risk and reduces trust.

16. What information should funders and leaders of CVI organizations consider for program compliance?

Governance oversight should ensure that written confidentiality protections are in place, law enforcement boundaries are clearly defined, disclosures are transparent, policies prioritize participants, and compliance reviews occur regularly. Proactive compliance strengthens credibility and partnerships.

17. What should programs do if trust has been damaged?

If trust has been damaged, programs should immediate work to clarify roles, conduct independent reviews of practices, reinforce safeguards, and engage in community listening sessions. Accountability efforts should focus on restoring trust rather than assigning blame or punishment.

18. How should CVI programs approach the use of Artificial Intelligence?

Artificial intelligence (AI) refers to tools that analyze data and generate patterns, summaries, classifications, or recommendations. In CVI contexts, AI may appear in data analytics platforms that identify trends, risk scoring or predictive modeling tools, grant reporting dashboards, administrative systems that summarize reports, or vendor proposals described as "smart," "automated," or "evidence-based." AI is not an intervention. At most, it is a tool that may inform decisions. For that reason, adopting AI is a governance decision rather than merely a technical upgrade.

Organizations should first ask what specific harm the tool is intended to reduce and whether AI is truly necessary or is substituting for relationship-based prevention work.
Organizations should also consider whether the AI tool aligns with public health principles and whether its use could **unintentionally introduce bias**, **surveillance concerns**, or **inequitable impacts**. Prevention focuses on reducing harm and strengthening protective factors, not predicting individual behavior. If an AI tool shifts toward classification, prediction, or enforcement-adjacent functions, it may conflict with prevention-centered values. Choosing not to adopt a particular AI tool is a valid and defensible public health decision.

19. What safeguards should apply if AI tools are used?

If AI-enabled tools are adopted, the same confidentiality, firewall, and consent principles described above apply equally to AI systems. Data collection should remain limited to what is necessary for program operations, and participant data should not be repurposed beyond its stated and disclosed use. Law enforcement should not have access to AI-generated outputs, and AI systems should never function as intelligence-gathering tools under the banner of prevention. AI tools must operate as decision-support tools rather than decision-makers. Professional judgment must be preserved, and staff should have clear authority to accept, modify, or reject automated outputs without consequence. Risk scores or classifications should not become fixed labels or be shared across systems in ways that influence enforcement, eligibility, or sanctioning decisions. Prevention-centered work must remain voluntary, relational, and subject to human review. Organizations should establish governance safeguards before using AI tools. These safeguards should address data ownership, access controls, records retention and deletion policies, bias monitoring and mitigation procedures, documentation of decision authority, and exit protocols in the event the organization disengages from the tool.

20. What should organizations disclose about AI use?

As stated throughout these FAQs, transparency is critical to maintaining participant trust. If participant data is used in AI systems, even for internal analysis, organizations should clearly explain what tools are being used, what data is included, what decisions the tool informs, and whether outputs may affect service delivery or resource allocation. Participants should not later discover that automated systems influenced decisions about them. When evaluating vendors or cross-agency initiatives involving AI, organizations should seek clear information regarding the evidence supporting the tool's use in prevention contexts, how bias or disparate impact has been assessed and mitigated, whether outputs can be explained in plain language, who is responsible for decisions informed by the tool, whether staff may override outputs without consequence, and whether the organization can disengage and ensure proper data deletion upon exit. Transparency must be ethically sufficient, not merely legally sufficient. Even when legally permissible, tools that erode trust can undermine violence prevention outcomes.

BEST PRACTICES CHECKLIST

Organizations should be able to answer affirmatively to each of the following:

- ☐ Participants are informed whether law enforcement partnerships and affiliations exist.
- ☐ Staff disclose law enforcement partnerships and affiliations.
- ☐ Participant data and identifying information is never shared without informed, voluntary participant consent or in accordance with a specific legal requirement.
- ☐ Intake forms clearly and accurately explain the limits of confidentiality.
- ☐ Law enforcement personnel does not have access to participant files.
- ☐ Written memoranda of understanding clearly define the roles and boundaries among program partners and any participating law enforcement personnel.
- ☐ The organization collects only the data that is necessary for its work.
- ☐ Policies (*e.g.*, information security and data privacy policy and records retention policy) are formally adopted, consistently implemented, and followed in practice.

ADDITIONAL REFERENCE MATERIALS

- NCJR, Discussion *Paper for Offices of Violence Prevention: Public Health- and Data Governance-Informed Considerations for the Use of Artificial Intelligence*.

ECVN is providing this resource for educational and informational purposes only. This document does not constitute legal advice and should not be relied upon as such. Organizations seeking legal advice should consult qualified legal counsel.