How Tracking Systems Place Victims at Risk

Homeless Management Information Systems & Victims of Abuse and Stalking

In 2001, the U.S. Congress directed the U.S. Department of Housing and Urban Development (HUD) to collect data on the extent of homelessness at a local level. The directive was intended to make an unduplicated count of homeless persons, to analyze use of assistance, to determine how people enter and exit homeless assistance systems, and to determine the effectiveness of such systems. Computer databases were suggested as one way to collect such data. Broadly interpreting this directive, HUD proposed federal standards to require HUD-funded entities to implement local Homeless Management Information Systems (HMIS) for collecting, tracking and sharing comprehensive personal data.

The National Network to End Domestic Violence (NNEDV) has been working closely with HUD, state coalitions, local programs, and allied groups to raise awareness of the privacy, safety, and security issues that HMIS raises for victims of abuse and stalking. NNEDV's *Safety Net: The National Safe & Strategic Technology Project* addresses all technology issues regarding victims and their advocates. The *Safety Net Project* is actively discussing alternative ways HUD can achieve Congress' intent while protecting victim safety and privacy. The Project continues to hear and discuss numerous risks to survivors while presenting national, state, and local data safety trainings and participating in national, state, and community level meetings relevant to victims and data collection.

Proposed Standards released in July 2003: HUD issued proposed HMIS standards to guide the formation of HMIS at local levels. These proposed standards direct local and state-wide Continuums of Care (CoCs) to establish databases containing client-identifying information and the current location of an individual within the service system and to retain this sensitive data for at least 7 years. HUD proposed a data standard for all local HMIS that requires all clients to be asked for personal identifying information, including name, date of birth, and Social Security number, when seeking transitional housing, emergency shelter or other support services such as food banks. The proposed standards encourage, but do not require, sharing of case notes across service providers within the continuum. Since many states are considering implementing state-wide HMIS systems, sensitive client-identified information, location, and case notes could be shared with every participating provider in a state. Sharing of data is at the discretion of each CoC.

In response to data confidentiality, safety, and security concerns voiced by advocacy organizations, HUD has made certain confidentiality exceptions for victims of domestic violence seeking shelter or housing assistance, and exempts participation in local HMIS if sharing information raises significant risk to clients of a domestic violence shelter, or victims accessing a non-domestic violence service provider. Given the lethal risk to victims, domestic violence and other organizations should not submit any client-identified data to HMIS servers.

In September 2003, NNEDV submitted comments responding to and citing multiple concerns with the proposed standards. NNEDV suggested that HUD follow alternative methods to collect data that provide less invasive means to obtain an unduplicated count of homeless individuals. NNEDV has strongly encouraged HUD to reconsider several aspects of the data collection methodology and security protocols proposed for HMIS implementation.

Many organizations submitted comments to HUD prior to the September 22, 2003 deadline. After considering these comments, HUD will release final standards sometime in 2004. At a July 2003 National Conference on Homelessness, HUD staff explained that they expect some providers in each continuum to be reporting some data by October 2004, but do not expect all service providers to be submitting data by then.

HUD Proposed Standards: www.hud.gov/offices/cpd/homeless/rulesandregs/fr4848-n-01.pdf

NNEDV Comments: www.nnedv.org/pdf/HMIS9_03.pdf

Safety and Privacy Risks for Victims:

1. **HUD can achieve its goal of obtaining an unduplicated count of homeless individuals with less invasive and less costly methods that offer greater protection for victims.** A point-in-time count of homeless individuals will achieve Congress' intent and offer greater protection to victims of abuse and stalking.
2. **In the proposed standards, HUD's exemption of domestic violence shelters from reporting requirements is insufficient.** NNEDV recognizes that HUD has included an exemption of domestic violence shelters from HMIS reporting requirements. While the exemption is a step in the right direction, it does not go far enough to adequately protect victims of abuse and stalking.
3. **The data standards set forth in HUD's proposal are overly broad and unnecessarily invasive, putting victims at risk.** The overwhelming breadth of information sought through HMIS, from social security number to medical diagnosis, is not required by Congress to get an unduplicated count of homeless individuals in the United States.

4. **HUD's proposed data standards should be a ceiling, not a floor.** NNEDV appreciates that HUD recognizes data confidentiality, safety, and security concerns, and as a result, has made certain confidentiality exceptions for victims of domestic violence, however some states are not honoring the safety intent of HUD and are pressuring local programs to compromise the safety of their clients or risk losing funding.
5. **In its proposed form, HMIS amounts to a homeless tracking and surveillance system.** Client-identified data would track a victim from location to location and from provider to provider. For victims of abuse and stalking, location information could be lethal. An unduplicated count and an anonymous database analyzing trends would meet the U.S. congressional directive without compromising privacy and safety.
6. **The collection of information regarding physical and behavioral health status is not relevant to HUD's goals.** Intake workers at many service providers are predominantly volunteers who are not trained to make medical and mental health assessments. HUD has no provisions in its proposed standards for prohibiting future use or misuse of HMIS data. As a result, erroneous information could become vulnerable to subpoena and could be misused in custody or family law matters.
7. **Informed consent for victims in crisis is nearly impossible.** Victims needing shelter are in a state of emergency. One recent survey of women in local shelters found that during shelter intake, many would have consented to share personal data in HMIS solely because they'd fear being denied shelter. Duress is not informed consent. For real consent, a victim needs time to review a list of every participating agency and any other entity with access to HMIS data, think about where her abuser works, who her abuser knows that may have a connection to a participating agency, and any other risks to sharing her location and data. She also needs the option to retract consent and be quickly deleted from the system. Victims face enough obstacles when fleeing violence and don't need these additional burdens.

> As one woman in shelter stated:
> *"I would not feel comfortable saying no to the people that are helping me. I'd believe this information would be needed in order for me to stay in shelter."*

8. **HUD's proposed standards encourage additional information sharing, which increases the likelihood that sensitive information will be compromised.** The proposed standards make it clear that while information sharing between providers is not required, it is encouraged. Widespread information sharing will place many victims in grave danger. Whenever sensitive information about a victim is shared between agencies, the security of that information is compromised due to the increasing number of people authorized to access the information, and increased risks of unauthorized access and hacking.
9. **HUD's proposed data security standards do not provide enough protection for sensitive information regarding victims of domestic violence.** FBI and independent security firm studies show that extensive security breaches are happening even in private corporations with highly funded, skilled information security departments. Communities implementing HMIS with non-profit and government resources have far less capacity to protect from intrusion the sensitive data stored at the service provider and also stored in HMIS servers.
10. **The proposed standards do not account for situations when an abuser works or volunteers for a HMIS provider, vendor, county or state government office.** In some states, hundreds of agencies and their staff will be authorized users of the HMIS systems. Since perpetrators and stalkers work in all fields, compiling and sharing client-identifiable data is inherently dangerous for victims.

~~~~~~~~~~~~~~~~~~ *Help Protect the Safety and Privacy of Victims* ~~~~~~~~~~~~~~~~~~

Strategies for addressing HMIS:

- Help state/local advocacy programs organize & educate about privacy, safety, & security concerns of HMIS.
- Find community allies from privacy, homeless, HIV/AIDS, mental health, and substance abuse organizations.
- Include local and state advocates, privacy and security advocates, attorneys, and academic experts on ethical research in any committees planning the implementation of HMIS.
- Work creatively with Continuums of Care to find ways to participate in HMIS without providing client-identified data. Encourage continuums to exempt domestic violence programs and all victims of abuse and stalking from present participation in HMIS, at least until HUD releases final federal HMIS standards.
- Work with HMIS committees to ensure that security for any system matches that of banking and FBI databases.

Resources & Assistance:

1. Contact your state coalition to discuss safety and privacy concerns, creative participation in HMIS for victims of abuse and stalking, and ways to educate your communities about safety and privacy risks.
2. Read NNEDV's comments on the Proposed HMIS Standards at www.nnedv.org under "Legal Action Center".
3. Contact NNEDV's Safety Net Project when you need to discuss further the privacy, safety, and security risks with HMIS and other information sharing and data tracking systems.