ELECTRONIC PRIVACY INFORMATION CENTER

Homeless Tracking Fact Sheet

Homeless Management Information Systems (HMIS) are database systems intended to track recipients of benefits in order to assess the number of persons receiving care, and to improve efficiency of services to the poor.

While well intentioned, proposed mandatory guidelines for these systems issued by the Department of Housing and Urban Development (HUD) are highly privacy-invasive.[1] Under the guidelines, federally-funded entities that provide support for the poor will have to:

- Collect extensive amounts of personally-identifiable information from everyone who receives care. Support centers will have to collect: full legal names, dates of birth, Social Security Numbers, ethnicity and race, gender, veteran status, and the person's residence prior to program entry.
- Collect other sensitive information from those who receive care: The HMIS questionnaire delves deeply into the personal lives of the homeless, tracking where they have been, what services they have used, their income, benefits, disabilities, health status, pregnancy status, HIV status, behavioral health status, education, employment, and whether they have experienced domestic violence.
- Collect information on individuals who seek care during a brief episode of their lives. For instance, individuals who sought shelter during the recent blackouts in the Northeast would be tracked by the system.
- Store this information for at least seven years.
- Report it regularly to central servers (in the state or region).

The risks to privacy and civil liberties of such a system include:

- **The potential development of a nationwide system of homeless tracking.** HUD's guidelines are meticulous in specifying requirements that could facilitate a future nationwide system of homeless registration and tracking. For instance, all data in the tracking system must be exportable to a universal data format. This system could be used to purge the homeless when they are unwanted in an area for political reasons.
- **Police Access to the HMIS Database is Nearly Unlimited.** HUD's proposed guidelines allow systems users to disclose information from the database for national security purposes without any showing of an emergency, a court order, or even a risk of attack. Secret Service access is similarly broad. Under the guidelines, agents from national security or the Secret Service could simply ask for an entire HMIS database and receive it lawfully. Law enforcement access is more limited, but nevertheless, HUD is not requiring police to obtain a warrant or court order before releasing HMIS data.

[1] Proposed guidelines available at http://www.epic.org/privacy/poverty/hmis.pdf.

- **HMIS imposes substantial computer security risks on the homeless.** Almost all of the database software reviewed by a HUD-sponsored study runs on standard, general-purpose computers using off-the-shelf consumer operating systems. One software implementation makes HMIS data available over the Internet with Microsoft IIS, a server program that has been plagued by malicious exploits. Another implementation appears to lack an audit trail, one of the most basic security precautions. In any case, when personal data is collected in one place, it creates heightened incentives for malicious crackers to attack the database.
- **HMIS places victims of domestic violence at heightened risk.** Those who are fleeing violent partners should not have their information collected or transmitted to any central computer to better protect their location and safety. HMIS could have the effect of allowing abusive partners to locate victims through access to the database (by law enforcement officers or HMIS users).
- **HMIS, if implemented, could gravely harm individuals living with HIV or AIDS.** The proposed guidelines call for collection of highly sensitive information. Accidental or deliberate exposure of information in the system could subject populations to stigma or discrimination. Additionally, these systems create a honey pot of data for divorce attorneys and others who will seek to use the information in custody and family law proceedings.

We urge the public to comment on HMIS.

- HUD should seek less-invasive alternatives to HMIS. Rather than building personally identifiable dossiers on every person who receives services, HUD could employ a census-style "snapshot." A snapshot of representative samples of the homeless population would serve the same purpose of obtaining a count, be less privacy invasive, and less expensive than HMIS.
- Law enforcement access should be curtailed. Access should only be granted pursuant to court order, warrant, or where exigent circumstances are present.
- Victims of domestic violence should not have to submit personal information to HMIS at a domestic violence shelter or through any service provider in the community.

One can comment until September 22, 2003 by submitting mail to the following address. There are no provisions for electronic or fax submissions.

Michael Roanhouse
Re: Doc. No. FR 4848-N-01 / HMIS Data
Office of Special Needs Assistance Programs
Office of the Assistant Secretary for Community Planning and Development
Room 7262 HUD
451 7th St. SW
Washington, DC 20410

For more information, contact EPIC:
Chris Jay Hoofnagle
Deputy Counsel
1718 Connecticut Ave. NW 200
Washington, DC 20009
hoofnagle@epic.org

For more information about domestic violence and HMIS, contact:
Cindy Southworth
Director of Technology
National Network to End Domestic Violence
safetynet@nnedv.org