



Demystifying HUD's HMIS Domestic Violence "Clarification"

October 20,
2004

Highlights at a Glance:

- In both their 10/1/04 FAQ and their 10/15/04 Clarification, HUD specifically says that there is **NO STATED DEADLINE** for domestic violence programs to begin submitting victim information. **Therefore, NO Continuum of Care (CoC) should pressure any Domestic Violence (DV) program to sign any contract or submit any data.** CoC's are encouraged to meet with DV programs to discuss these complex safety risks, but no DV program data sharing is required at this time.
- HUD's 10/15/04 Clarification recognizes that state confidentiality laws may trump the HMIS regulation and expresses that in the event that state laws conflict with HUD's Final HMIS Notice, **state law will prevail.**
- Although it is still **insufficient protection for DV victims**, the 10/15/04 Clarification does declare HUD will **not require submission of victim name and Social Security Numbers** from DV programs to a CoC.
- **HUD has still NOT reinstated their previously granted and vital DV exemption** for domestic violence programs and individual victims that is cited on page 43435 of HUD's Proposed HMIS Standards.
- HUD's 10/15/04 Clarification **does not ensure any safety and privacy protections for DV victims that use other community based services** such as food banks and homeless shelters.
- HUD'S 10/15/04 clarification **still requires domestic violence programs to collect universal data elements as part of a client's record which includes: date of birth, ethnicity and race, gender, and disabling condition.** These universal elements, when kept in an individual client's record, can make victims highly identifiable and compromise anonymity.
- Though masked by complex technical terms, the 10/15 **Clarification requires a victim's unique identifiers** (Date of Birth, etc) to be submitted by HUD-funded DV programs to a central HMIS server, **resulting in every victim being linked and identifiable at the central server.** This violates the core promise of confidentiality that DV shelters and advocates make to all victims. Any submission of a victim's unique identifiers to HMIS will continue to place victims in danger.
- HUD has **not yet responded** to the Administrative Appeal that NNEDV filed on Aug. 27, 2004.
- These HUD documents **DO NOT PROTECT victims** from: abusers who work in the system; public records requests to access an HMIS database; real or impersonated law enforcement access (P. 45929 of Final Notice); and, common-place security breaches caused by internal authorized users (studies show 75-90% of all security breaches occur internally).

This Handout Addresses HUD's HMIS Clarification released on October 15, 2004: This "Clarification" attempts to address protections for victims, but continues to endanger victims of domestic violence. HUD's HMIS Clarification is linked at www.nnedv.org/hmis

Note: This handout is a companion piece to the NNEDV's Domestic Violence Advocacy Guide to the Final HMIS Standards available at: www.nnedv.org/hmis This handout discusses new developments, while the Advocacy Guide provides background information and an in-depth analysis of the HMIS Final Standards released July 30, 2004.

Direct Excerpts from HUD's 10/15/04 "Clarification"	What this means for victims and their advocates
<p>"HUD supported the development of local HMIS in response to Congressional direction on the need for improved data on and the analysis of the extent of homelessness and the effectiveness of the McKinney -Vento Act programs including: (1) production of an unduplicated count of clients served at the local level; (2) analysis of patterns of use of people entering and exiting the homeless assistance system; and (3) evaluation of the effectiveness of the homeless assistance system" (Page 2).</p>	<p>Congress does NOT direct or require a human tracking system. In the 2001 Conference Committee report (which is not federal law), Congress asked HUD to get a better count and analyze patterns and effectiveness.</p> <p>HUD chose to create a human tracking system . This HMIS system creates lethal risks by sharing personal identifiable information about victims of domestic violence.</p> <p>There are many less-invasive, less dangerous, and less expensive ways to meet this directive.</p>
<p>"Broad-based participation of all homeless service providers at the local level in HMIS and the collection of longitudinal data are critical to meeting this directive" (Page 2).</p>	<p>HMIS is a longitudinal research project, which will track people for 7 years and share individual people's data across cities and states.</p> <p>Many university research ethics boards would raise grave concerns about the complete lack of informed consent in HMIS data collection. Several surveys of DV victims, reinforce significant concerns that homeless persons and many DV victims may feel compelled provide data to HMIS, believing they will not otherwise obtain services.</p>
<p>"Domestic violence programs play a critical role in many Continuums of Care (CoC) and constitute a large proportion of shelter beds and homeless service slots. Their absence from participation in an HMIS would prevent these communities from obtaining an unduplicated count of homeless persons in their community or understanding adequately the needs of the homeless population, including victims of domestic violence" (Page 2).</p>	<p>It is possible to obtain an unduplicated count of homeless persons by conducting weekly or monthly coordinated "point-in-time" counts. On the same day at the same time, every shelter could count their residents and provide rich anonymous demographics. Since homeless persons cannot be in two shelters at once, HUD could have an unduplicated count and rich qualitative data.</p>
<p>"A distinction is made between (1) data that domestic violence providers collect from homeless persons and (2) data that domestic violence providers submit to a central server in order to produce an unduplicated count of homeless persons at the CoC level" (Page 3).</p>	<p>For over 20 years, DV programs have been collecting (and carefully protecting) unduplicated data and only sharing aggregate data with federal, state, & local funders.</p> <p>This is the first attempt of any U.S. federal domestic violence shelter funder to require local DV shelters to submit victim data to central servers. HUD's requirement violates a core promise of confidentiality that is necessary for DV victims to feel and be safer in getting help.</p>
<p>"HUD recognizes that communities and domestic violence programs need time to develop and implement methods to effectively address domestic violence provider participation in HMIS and, therefore, permits CoCs to stage the entry of domestic violence programs last, including the later staging of domestic violence after the October 2004, goal for HMIS implementation providers will not affect HUD' s assessment of CoC progress in HMIS implementation in the national CoC competitive ranking process" (Page 4).</p>	<p>This means that currently local and state Continues of Care (CoCs) should not be pressuring domestic violence programs to submit any victim data or threatening to withhold any funding.</p> <p>HUD continues to specify that there is NO STATED DEADLINE for domestic violence participation.</p>
<p>"The Final Notice also recognizes stronger state confidentiality provisions. In the event that state laws conflict with the Final Notice, as determined by an appropriate state government entity, state law will prevail (see Section 4 of the Final Notice)."</p>	<p>The 7/30 Final HMIS Standards say that CoCs "must also comply with federal, state and local laws that require additional confidentiality protections." Pg 45928</p> <p>Several state coalitions have sent legal memos to HUD demonstrating successfully that their state confidentiality laws prohibit DV advocates from sharing client-level data.</p> <p>Federal laws such as VOCA and FVPSA are being analyzed since they may prohibit submitting victim data to HMIS.</p>
<p>"Accordingly, domestic violence programs that receive McKinney-Vento funds must collect the universal and program-specific data elements required for reporting. HUD does not require domestic violence providers to collect or report an address for a client served by a domestic violence provider" (Page 5).</p>	<p>The present exemption of name, social security number and last permanent address is insufficient to ensure safety because HUD's universal data elements still include date of birth, ethnicity and race, gender, and disabling condition. These universal elements make victims highly identifiable and do not provide sufficient anonymity vitally needed for safety.</p> <p>By merely knowing which shelter a victim has fled to or which town she now lives in, an abuser can use a combination of the other HMIS data elements to identify her, track her down and harm her.</p>

Direct Excerpts from HUD's 10/15/04 "Clarification"	What this means for victims and their advocates
<p>"HUD understands the concerns regarding submission of client-identified data from domestic violence programs to a central location. HUD will not require the submission of personal identifiers (name and Social Security Number (SSN) from these programs to the CoC"(Page 5).</p>	<p>HUD is still requiring that DV programs compromise victim confidentiality and safety by submitting client-level data AND unique identifiers on every victim.</p> <p>HUD is still requiring that Date of Birth be shared – an EXTREMELY accurate unique identify used for years to match up clients and victims across the country.</p>
<p>Domestic violence programs can choose to use a proxy, coded, encrypted, or hashed unique identifier - in lieu of name and SSN - that is appended to the full service record of each client served and submitted to the central server at least once annually for purposes of unduplication and data analysis" (Page 5).</p>	<p>Coded, Encrypted, and Hashed... these terms all indicate a "scrambling" of her data at the DV shelter and allow HUD to unscramble (decode, unencrypt, etc) her confidential information at the central server. Therefore none of these technology protections would actually protect her identity.</p>
<p>"The coded unique identifier would need to include, but is not limited to, characters and digits from a portion of a client's name, date of birth, and gender. This unique identifier can be generated either manually or through the use of an advanced technological encryption algorithm" (Page 6).</p>	<p>HUD is dictating the elements needed for creating unique identifiers so that victim's confidential information can be linked at the central server and she can be tracked across the city or state.</p> <p>HUD is not allowing local DV shelters to randomly create an ANONYMOUS unique identifier that is not connected to her name, date of birth, social security number, or other details.</p>
<p>"HUD fully supports alternative methods of participation by domestic violence providers. Domestic violence programs are charged to meet with CoC representatives to identify administrative solutions, such as delaying entry of data into the HMIS until after the client has exited the domestic violence program, or other technological or administrative solutions that adequately protect data and allow for an accurate unduplicated count of homeless persons and analysis of homeless data throughout the CoC to meet the goals of the congressional directive" (Page 6).</p>	<p>Given that it is possible to meet the congressional directive to get a better unduplicated count and analyze trends, DV programs should be allowed to participate in regular and coordinated "Point-in-Time" Counts across that could provide unduplicated counts across entire time-zones without expensive and dangerous human tracking systems.</p> <p>Domestic violence programs should be allowed to provide their Continuum of Care with aggregate totals - and nothing further.</p>
<p>"HUD recognizes that the privacy and security concerns of domestic violence victims are unlike those of other homeless clients. In response to these concerns, HUD has developed HMIS privacy and security standards that are improvements to current practices, set high baseline standards for all users of HMIS data, and adequately protect personal information collected from domestic violence victims as well as all homeless clients" (Page 6).</p>	<p>This remains confusing since in the proposed HMIS standards released July 22, 2003 HUD recognized the risks to victims and provided a critical domestic violence exemption. This previously granted exemption allowed domestic violence programs to submit only aggregate totals and also allowed individual victims using other community services (food banks, etc) to keep their life-threatening data out of HMIS databases.</p>
<p>"As stated in the Final Notice, the baseline privacy and security standards are based on principles of fair information practice and on security standards recognized by the information The privacy standards were developed after careful review of technology and privacy communities" (Page 7).</p>	<p>The "Fair Information Principles" (FIPs) are widely accepted and require far more privacy protections than reflected in the Final HMIS Standards or Clarification.</p> <p>Learn more about FIPS at: www.privacyjournal.net/bio.htm</p>
<p>"For some key provisions in the HMIS privacy standards, HUD set baseline standards that exceeded those in HIPAA, especially for provisions that are important to domestic violence programs" (Page 7).</p>	<p>Since DV shelters were founded over 30 years ago, advocates have observed confidentiality practices far more stringent than new HIPAA requirements. HMIS continues to allow access to victim information with merely a verbal request from law enforcement or those pretending to be law enforcement.</p>

Direct Excerpts from HUD's 10/15/04 "Clarification"	What this means for victims and their advocates
<p>"HUD also developed multi-layered security provisions that meet or surpass current Information Technology (IT) industry standards requiring: (1) user authentication; (2) industry standard encryption (128-bit Secure Socket Layer) of all HMIS data that are electronically transmitted over the Internet, publicly accessible networks, or phone lines; and (3) strict limitations to physical and network access to systems with HMIS data. In addition to these baseline standards, HUD recommends additional privacy and security standards that CoCs and programs could implement to further increase the security of the system" (Page 7).</p>	<p>All of these technological elements can be breached by</p> <ol style="list-style-type: none"> Internal User error – since FBI and private sector studies show that over 75% of security breaches are internal, no level of encryption or firewall will ensure a level of victim data confidentiality vitally needed for safety. Real (or Impersonated) Law Enforcement Access -- Since HUD allows law enforcement access with merely a verbal (or telephone) request. Public Records Requests – since these databases are created with public government funds, a Freedom of Information Act (FOIA) request could compromise victim information. Internal abusers who work for the system or know someone who has access -- perhaps through a non-profit, government entity, or system administrator.
<p>"The baseline privacy and security standards for HMIS required by the Final Notice far exceed the requirements for many other systems into which these client data are entered. HUD continues to encourage organizations to apply these additional protections as they deem appropriate" (Page 7).</p>	<p>Victim-identifying information collected by domestic violence shelters has always been private information – never shared with other agencies in the community or funders except as aggregate totals.</p> <p>Due to extreme safety needs, too many victims of domestic violence cannot use other services which track or share their data, such as TANF. If HUD requires victims to be entered into large tracking systems, some victims will not be able to use critical and life-saving shelters or other services.</p>
<p>"Other methods currently in use include delayed entry of data into the HMIS until after the client has exited the program or HMIS system administration/hosting by the domestic violence provider agency" (Page 8).</p>	<p>Many victims flee to a domestic violence shelter and then settle in that community. Since a large part of abuse includes isolating a victim and her children from all community supports, it is important for victims to leave the shelter, but stay in the same community: attending weekly support group, utilizing transitional housing programs, and keeping the children in the same school.</p> <p>Also, "separation violence" and stalking occur at separation, and continue long after she has fled. Entering data about her location after she exits a shelter is a false sense of security.</p>

Resources & Assistance:

- Contact your state coalition to discuss:
 - What to do if HMIS Administrators pressure local programs to compromise safety and confidentiality.
 - Possible local, state, or federal laws that may preempt HMIS requirements.
 - Ways to educate survivors about safety and privacy risks and their rights not to share data.
- Read NNEDV's materials on HMIS at www.nnedv.org/hmis
- 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. Email SafetyNet@nnedv.org
- Continue to protect the confidentiality of all victims and inform survivors about these tracking systems and their rights.

"DV Exemption" language from HUD's Proposed Standards page 43435

"At a minimum, HUD will not expect a domestic violence shelter it funds to participate in a local HMIS where HMIS software or data protocols raise a significant risk to its clients. In addition, providers of homeless assistance services will not be required to report personal identifying information for victims of domestic violence or for people in witness protection programs to a central storage facility given the unique concerns about personal safety for these populations. However, providers will be expected to provide unduplicated project-level data about participant characteristics without personal identifiers."